

VMware vRealize Log Insight- Administratorhandbuch

vRealize Log Insight 2.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter

<http://www.vmware.com/de/support/pubs>.

DE-001659-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

<http://www.vmware.com/de/support/>

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2014 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

VMware, Inc.

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.

Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Informationen zum vRealize Log Insight-Administratorhandbuch 5

1 Verwaltung von Log Insight 7

- Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance 8
- Ändern der Netzwerkeinstellungen der vApp für Log Insight 9
- Zuweisen einer permanenten Lizenz zu Log Insight 9
- Upgrades aus früheren Versionen von Log Insight 10
- Verwalten eines Log Insight -Clusters 13
- Aktivieren des integrierten Lastenausgleichsmoduls 18
- Prüfen des Systemzustands der virtuellen Log Insight -Appliance 19
- Überwachen von Protokollereignisse sendenden Hosts 21
- Überwachen des Status von Log Insight Windows und Linux Agents 22
- Verwalten von Benutzerkonten in Log Insight 22
- Übersicht über den Log Insight Windows Agent 28
- Übersicht über den Log Insight Linux Agent 45
- Fehlerbehebung in den Log Insight Agents 54
- Konfigurieren von Log Insight -Systemwarnungen 61
- Synchronisieren der Uhrzeit der virtuellen Log Insight -Appliance 67
- Konfigurieren des SMTP-Servers für Log Insight 68
- Integration von Log Insight in andere VMware-Produkte 69
- Aktivieren oder Deaktivieren der Datenarchivierung in Log Insight 85
- Aktivieren der Benutzerauthentifizierung über Active Directory 86
- Installieren eines benutzerdefinierten SSL-Zertifikats über die Log Insight -Web-Benutzeroberfläche 88
- Ändern des Standard-Zeitlimits für Log Insight -Websitzungen 94
- Format der Log Insight -Archivdateien 95
- Importieren eines Log Insight -Archivs in Log Insight 95
- Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON 96
- Konfigurieren der Log Insight -Ereignisweiterleitung mit SSL 97
- Hinzufügen eines Ziels für die Log Insight -Ereignisweiterleitung 97
- Neustart des Log Insight -Dienstes 98
- Ausschalten der virtuellen Log Insight -Appliance 99
- Hinzufügen von Arbeitsspeicher und CPU zur virtuellen Log Insight -Appliance 99
- Einstellen des Versands von Protokollierungsdaten an VMware 100

2 Fehlerbehebung bei Log Insight 101

- Es gehen keine ESXi-Protokolle mehr in Log Insight ein 101
- Log Insight steht zu wenig Festplattenspeicher zur Verfügung 102
- Herunterladen eines Support-Pakets für Log Insight 103
- Erstellen eines Support-Pakets von Log Insight über die Virtual Appliance-Konsole 103
- Zurücksetzen des Admin-Benutzerkennworts 104
- Zurücksetzen des Root-Benutzerkennworts 104

Warnungen konnten nicht an vRealize Operations Manager gesendet werden	105
Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich	106
SMTP funktioniert bei aktivierter STARTTLS-Option nicht	106
Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann	107
Fehlschlagen des Upgrades mit einem internen Serverfehler	108

Index	109
-------	-----

Informationen zum vRealize Log Insight-Administratorhandbuch

Das *VMware vRealize Log Insight*-Administratorhandbuch enthält Informationen über die Verwaltung von Log Insight und beschreibt unter anderem die Verwaltung von Benutzerkonten, die Integration in andere VMware-Produkte und die Fehlerbehebung bei den gängigsten Problemen.

Zielgruppe

Die vorliegenden Informationen richten sich an Benutzer, die Log Insight verwalten möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

Verwaltung von Log Insight

Administratorbenutzer können im Verwaltungsabschnitt der Web-Benutzeroberfläche von Log Insight Standardverwaltungsaufgaben ausführen.

Bestimmte Änderungen an der Konfiguration von Log Insight werden erst nach einem Neustart des loginsight-Diensts übernommen. Änderungen, die die Uhrzeitkonfiguration, die vSphere-Integration und die Authentifizierung betreffen, erfordern keinen Neustart.

Dieses Kapitel behandelt die folgenden Themen:

- [„Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“](#), auf Seite 8
- [„Ändern der Netzwerkeinstellungen der vApp für Log Insight“](#), auf Seite 9
- [„Zuweisen einer permanenten Lizenz zu Log Insight“](#), auf Seite 9
- [„Upgrades aus früheren Versionen von Log Insight“](#), auf Seite 10
- [„Verwalten eines Log Insight-Clusters“](#), auf Seite 13
- [„Aktivieren des integrierten Lastenausgleichsmoduls“](#), auf Seite 18
- [„Prüfen des Systemzustands der virtuellen Log Insight-Appliance“](#), auf Seite 19
- [„Überwachen von Protokollereignisse sendenden Hosts“](#), auf Seite 21
- [„Überwachen des Status von Log Insight Windows und Linux Agents“](#), auf Seite 22
- [„Verwalten von Benutzerkonten in Log Insight“](#), auf Seite 22
- [„Übersicht über den Log Insight Windows Agent“](#), auf Seite 28
- [„Übersicht über den Log Insight Linux Agent“](#), auf Seite 45
- [„Fehlerbehebung in den Log Insight Agents“](#), auf Seite 54
- [„Konfigurieren von Log Insight-Systemwarnungen“](#), auf Seite 61
- [„Synchronisieren der Uhrzeit der virtuellen Log Insight-Appliance“](#), auf Seite 67
- [„Konfigurieren des SMTP-Servers für Log Insight“](#), auf Seite 68
- [„Integration von Log Insight in andere VMware-Produkte“](#), auf Seite 69
- [„Aktivieren oder Deaktivieren der Datenarchivierung in Log Insight“](#), auf Seite 85
- [„Aktivieren der Benutzerauthentifizierung über Active Directory“](#), auf Seite 86
- [„Installieren eines benutzerdefinierten SSL-Zertifikats über die Log Insight-Web-Benutzeroberfläche“](#), auf Seite 88
- [„Ändern des Standard-Zeitlimits für Log Insight-Websitzungen“](#), auf Seite 94

- „Format der Log Insight-Archivdateien“, auf Seite 95
- „Importieren eines Log Insight-Archivs in Log Insight“, auf Seite 95
- „Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON“, auf Seite 96
- „Konfigurieren der Log Insight-Ereignisweiterleitung mit SSL“, auf Seite 97
- „Hinzufügen eines Ziels für die Log Insight-Ereignisweiterleitung“, auf Seite 97
- „Neustart des Log Insight-Diensts“, auf Seite 98
- „Ausschalten der virtuellen Log Insight-Appliance“, auf Seite 99
- „Hinzufügen von Arbeitsspeicher und CPU zur virtuellen Log Insight-Appliance“, auf Seite 99
- „Einstellen des Versands von Protokollierungsdaten an VMware“, auf Seite 100

Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance

Die SSH-Verbindung zur virtuellen Appliance ist standardmäßig deaktiviert. Um SSH-Verbindungen zu aktivieren, müssen Sie das SSH-Root-Kennwort über VMware Remote Console konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Log Insight-Appliance bereitgestellt ist und ordnungsgemäß ausgeführt wird.

Vorgehensweise

- 1 Klicken Sie in der vSphere-Client-Bestandsliste auf die virtuelle Log Insight-Appliance und öffnen Sie die Registerkarte **Konsole**.
- 2 Rufen Sie mit der im Startbild angegebenen Tastenkombination eine Befehlszeile auf.
- 3 Geben Sie in der Konsole **root** ein und drücken Sie die Eingabetaste. Lassen Sie das Kennwort leer und drücken Sie die Eingabetaste.

In der Konsole wird folgende Meldung angezeigt: Kennwortänderung angefordert. Wählen Sie ein neues Kennwort.

- 4 Lassen Sie das alte Kennwort leer und drücken Sie die Eingabetaste.
- 5 Geben Sie ein neues Kennwort für den Root-Benutzer ein, drücken Sie die Eingabetaste, geben Sie das neue Kennwort für den Root-Benutzer erneut ein und drücken Sie die Eingabetaste.

Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Sie können dasselbe Zeichen nicht mehr als vier Mal wiederholen.

Es wird folgende Meldung angezeigt: Kennwort geändert.

Weiter

Sie können das Root-Kennwort verwenden, um SSH-Verbindungen zur virtuellen Log Insight-Appliance herzustellen.

Ändern der Netzwerkeinstellungen der vApp für Log Insight

Sie können die Netzwerkeinstellungen der virtuellen Appliance für Log Insight ändern, indem Sie die vApp-Eigenschaften in vSphere Client bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Bearbeiten von vApp-Eigenschaften verfügen.

Vorgehensweise

- 1 Schalten Sie die Log Insight-vApp aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Log Insight-vApp in der Bestandsliste und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **vApp-Optionen > IP-Zuteilungsrichtlinie**.
- 4 Wählen Sie eine Zuteilungsoption für IP-Adressen.

Option	Beschreibung
Fest	IP-Adressen werden manuell konfiguriert. Es wird keine automatische Zuteilung vorgenommen.
Vorübergehend	IP-Adressen werden beim Einschalten der vApp automatisch mithilfe von IP-Pools aus einem angegebenen Bereich zugeteilt. Die IP-Adressen werden freigegeben, wenn die Appliance ausgeschaltet wird.
DHCP	Zum Zuteilen der IP-Adressen wird ein DHCP-Server verwendet. Die vom DHCP-Server zugewiesenen Adressen sind in den OVF-Umgebungen von virtuellen Maschinen sichtbar, die in der vApp gestartet wurden.

- 5 (Optional) Wenn Sie **Fest** auswählen, klicken Sie auf **vApp-Optionen > Eigenschaften** und weisen Sie der vApp für Log Insight eine IP-Adresse, eine Netzmaske, einen DNS und einen Hostnamen zu.



VORSICHT Geben Sie nicht mehr als zwei Domännennamenserver an. Wenn Sie mehr als zwei Domännennamenserver angeben, werden alle konfigurierten Domännennamenserver in der virtuellen Log Insight-Appliance ignoriert.

- 6 Schalten Sie die vApp für Log Insight ein.

Zuweisen einer permanenten Lizenz zu Log Insight

Sie können Log Insight nur mit einem gültigen Lizenzschlüssel nutzen.

Wenn Sie Log Insight von der VMware-Website herunterladen, erhalten Sie eine Testlizenz. Diese Lizenz ist 60 Tage lang gültig. Nach Ablauf der Testlizenz müssen Sie eine permanente Lizenz erwerben, um Log Insight weiter nutzen zu können.

Im Verwaltungsabschnitt der Web-Benutzeroberfläche von Log Insight können Sie den Log Insight-Lizenzierungsstatus überprüfen und Ihre Lizenz verwalten.

Voraussetzungen

- Beziehen Sie über My VMware™ einen gültigen Lizenzschlüssel.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Wählen Sie unter „Management“ **Lizenz**.
- 3 Geben Sie im Textfeld **Lizenzschlüssel** Ihren Lizenzschlüssel ein und klicken Sie auf **Schlüssel festlegen**.
- 4 Stellen Sie sicher, dass der Lizenzstatus „Aktiv“ ist und dass Lizenztyp und Ablauftag korrekt sind.

Upgrades aus früheren Versionen von Log Insight

Der Upgrade-Vorgang fällt je nach installierter Version von Log Insight etwas anders aus.

Installierte Version	Upgrade-Version	Upgrade-Vorgang
Log Insight 1.0 GA und 1.5 TP1	Log Insight 1.5 GA	Weitere Informationen hierzu finden Sie unter „ Upgrade von Log Insight mithilfe der Befehlszeilenschnittstelle “, auf Seite 11.
Log Insight 1.5 TP2 und höher	Log Insight 1.5 GA	Weitere Informationen hierzu finden Sie unter „ Upgrade von Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche “, auf Seite 12.
Log Insight 1.5 GA	Log Insight 2.0 Beta	Siehe „ Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche “, auf Seite 12 und „ Aktualisieren eines Worker-Knotens in einem Log Insight-Cluster “, auf Seite 16
Log Insight 1.5 GA	Log Insight 2.0 GA im Clustermodus	1 „Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 12. 2 „Hinzufügen eines Worker-Knotens zu einem Log Insight-Cluster“, auf Seite 13
Log Insight 2.0 Beta Eigenständiger Knoten	Log Insight 2.0 GA	Siehe „ Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche “, auf Seite 12.
Log Insight 2.0 Beta Worker-Knoten	Log Insight 2.0 GA	Siehe „ Aktualisieren eines Worker-Knotens in einem Log Insight-Cluster “, auf Seite 16.
Log Insight 2.0 GA Eigenständiger Knoten	Log Insight 2.5 Beta	Siehe „ Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche “, auf Seite 12.
Log Insight 2.0 GA Worker-Knoten	Log Insight 2.5 Beta	Siehe „ Aktualisieren eines Worker-Knotens in einem Log Insight-Cluster “, auf Seite 16.
Log Insight 2.5 Beta Eigenständiger Knoten	Log Insight 2.5 GA	Siehe „ Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche “, auf Seite 12.
Log Insight 2.5 Beta Worker-Knoten	Log Insight 2.5 GA	Siehe „ Aktualisieren eines Worker-Knotens in einem Log Insight-Cluster “, auf Seite 16.

Upgrade von Log Insight mithilfe der Befehlszeilenschnittstelle

Da Log Insight 1.0 GA und 1.5 TP1 über keine Upgrade-Benutzeroberfläche verfügen, müssen Sie eine Befehlszeilenschnittstelle verwenden, um diese Versionen auf Log Insight 1.5 zu aktualisieren.

Verwenden Sie für Upgrades der Log Insight-Versionen 1.5 TP2 und höher die Verwaltungs-Benutzeroberfläche. Weitere Informationen hierzu finden Sie unter „[Upgrade von Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche](#)“, auf Seite 12.

In diesem Vorgang wird die Konsole der virtuellen Appliance verwendet, doch können Sie ihn auch über SSH ausführen.

HINWEIS Alle aktiven Benutzer der Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Achten Sie darauf, in der virtuellen Log Insight-Appliance das Root-Benutzerkennwort festzulegen, um SSH- und Konsolenvorgänge zu aktivieren. Weitere Informationen hierzu finden Sie unter „[Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance](#)“, auf Seite 8.
- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der RPM-Datei für das Log Insight-Upgrade-Paket an.

Vorgehensweise

- 1 Laden Sie die .rpm-Datei auf einen Host mit SSH-Zugriff auf die virtuelle Log Insight-Appliance herunter.
- 2 Verwenden Sie das Secure Copy Protokoll, um die .rpm-Datei auf die virtuelle Log Insight-Appliance zu kopieren.

Betriebssystem	Kommando/Werkzeug
Linux	<code>scp Pfad zur RPM-Datei/loginsight-cloudvm-version-log-insight-buildnumber.x86_64.rpm root@<LogInsightIPorHostname>:~</code>
Windows	Laden Sie für Windows-Systeme einen SCP-Client wie WinSCP herunter.

- 3 Verwenden Sie die vSphere-Client-Konsole, um sich als Root-Benutzer bei der virtuellen Log Insight-Appliance anzumelden.
- 4 Führen Sie den Befehl `service loginsight stop` aus.
- 5 Führen Sie den Befehl `rpm -Uvh loginsight-cloudvm-<version>-<log-insight-build-number>.x86_64.rpm` aus und warten Sie, bis die Aktualisierung abgeschlossen ist.
- 6 Führen Sie den Befehl `service loginsight start` aus.
- 7 Stellen Sie sicher, dass Sie sich bei der Web-Benutzeroberfläche von Log Insight anmelden können.



ERINNERUNG Das URL-Format lautet `https://log-insight-host`, wobei log-insight-host die IP-Adresse oder Hostname der virtuellen Log Insight-Appliance ist.

Wenn Sie eine Fehlerseite sehen, melden Sie sich als Root-Benutzer bei der Konsole der virtuellen Appliance an und führen Sie den Befehl `service loginsight restart` aus, um den loginsight-Dienst neu zu starten.

Upgrade von Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche

Administratoren können Log Insight 1.5 TP2 und höher mit der Verwaltungsbenutzeroberfläche aktualisieren.

HINWEIS Alle aktiven Benutzer der Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der RPM-Datei für das Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Appliance**.
- 3 Klicken Sie auf **RPM hochladen** und navigieren Sie zur RPM-Datei.
- 4 Klicken Sie auf **Upgrade durchführen**.
Log Insight lädt die RPM-Datei auf die virtuelle Appliance hoch und zeigt ein Bestätigungsfeld an.
- 5 Klicken Sie zwecks Bestätigung auf **Upgrade**.
- 6 Akzeptieren Sie die neue Endbenutzer-Lizenzvereinbarung (EULA), um das Upgrade abzuschließen.

Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche

Administratoren können Log Insight 1.5 GA und höher mit der Verwaltungsbenutzeroberfläche aktualisieren.

HINWEIS Alle aktiven Benutzer der Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der .pak-Datei für das Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Appliance**.
- 3 Klicken Sie auf **PAK hochladen** und navigieren Sie zur .pak-Datei.

- 4 Klicken Sie auf **Upgrade durchführen**.
Log Insight lädt die .pak-Datei zur virtuellen Appliance hoch und zeigt ein Bestätigungsdialogfeld an.
- 5 Klicken Sie zwecks Bestätigung auf **Upgrade**.
- 6 Akzeptieren Sie die neue Endbenutzer-Lizenzvereinbarung (EULA), um das Upgrade abzuschließen.

Weiter

Sie können eine neue Instanz der virtuellen Log Insight-Appliance bereitstellen und diese zum vorhandenen Log Insight-Knoten hinzufügen, um einen Cluster zu bilden. Der vorhandene Knoten wird zu einem Masterknoten und die neu bereitgestellte Log Insight-Instanz zum Worker-Knoten. Weitere Informationen hierzu finden Sie unter „[Hinzufügen eines Worker-Knotens zu einem Log Insight-Cluster](#)“, auf Seite 13.

Verwalten eines Log Insight -Clusters

Sie können über die Log Insight-Webschnittstelle Knoten in einem Log Insight-Cluster hinzufügen, entfernen und aktualisieren.

Hinzufügen eines Worker-Knotens zu einem Log Insight -Cluster

Stellen Sie eine neue Instanz der virtuellen Log Insight-Appliance bereit und fügen Sie sie einem vorhandenen Log Insight-Master-Knoten hinzu.

Vorgehensweise

- 1 [Bereitstellen der virtuellen Log Insight-Appliance](#) auf Seite 13
Laden Sie die virtuelle Log Insight-Appliance herunter. VMware verteilt die virtuelle Log Insight-Appliance als .ova-Datei. Stellen Sie die virtuelle Log Insight-Appliance mithilfe von vSphere Client bereit.
- 2 [Hinzufügen zu einer vorhandenen Bereitstellung](#) auf Seite 15
Nach Bereitstellung und Einrichtung eines eigenständigen Log Insight-Knotens können Sie eine neue Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen Log Insight -Cluster zu bilden.

Bereitstellen der virtuellen Log Insight -Appliance

Laden Sie die virtuelle Log Insight-Appliance herunter. VMware verteilt die virtuelle Log Insight-Appliance als .ova-Datei. Stellen Sie die virtuelle Log Insight-Appliance mithilfe von vSphere Client bereit.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der .ova-Datei der virtuellen Log Insight-Appliance verfügen.
- Vergewissern Sie sich, dass Sie über die Berechtigungen verfügen, die OVF-Vorlagen in der Bestandsliste bereitzustellen.
- Überprüfen Sie, ob Ihre Umgebung über genügend Ressourcen verfügt, um die Mindestanforderungen der virtuellen Log Insight-Appliance zu erfüllen. Weitere Informationen finden Sie im Abschnitt *Mindestanforderungen* der Anleitung *Erste Schritte für VMware vRealize Log Insight*.
- Die Dimensionierungsempfehlungen für die virtuelle Appliance müssen von Ihnen gelesen und verstanden werden. Weitere Informationen finden Sie im Abschnitt *Dimensionierung der virtuellen Log Insight-Appliance* der Anleitung *Erste Schritte für VMware vRealize Log Insight*.

Vorgehensweise

- 1 Wählen Sie in vSphere Client die Option **Datei > OVF-Vorlage bereitstellen**.

- 2 Folgen Sie den Eingabeaufforderungen im Assistenten zum Bereitstellen von OVF-Vorlagen.
- 3 Wählen Sie auf der Seite „Bereitstellungskonfiguration“ die Größe der virtuellen Log Insight-Appliance auf der Basis der Größe der Umgebung, für die Sie Protokolle erfassen möchten.

Klein ist die Mindestanforderung für Produktionsumgebungen.

Option	Protokollaufnahmerate	vCPUs	Arbeitsspeicher	IOPS	Syslog-Verbindungen	Ereignisse pro Sekunde
Extra klein	3 GB/Tag	2	4 GB	75	20	200
Klein	15 GB/Tag	4	8 GB	500	100	1000
Mittel	37,5 GB/Tag	8	16 GB	1000	250	2500
Groß	112,5 GB/Tag	16	32 GB	1500	750	7500

HINWEIS Wenn Sie **Groß** wählen, müssen Sie die virtuelle Hardware auf der virtuellen Maschine von Log Insight nach der Bereitstellung aktualisieren.

- 4 Wählen Sie auf der Seite „Festplattenformat“ ein Festplattenformat.
 - **Thick-Provision Lazy-Zeroed** erstellt eine virtuelle Festplatte im Standard-Thick-Format. Der für die virtuelle Festplatte erforderliche Speicherplatz wird dann zugeteilt, wenn die virtuelle Festplatte erstellt wird. Die Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt während der ersten Schreibvorgänge der virtuellen Appliance gelöscht.
 - **Thick-Provision Eager-Zeroed** erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.

WICHTIG Stellen Sie, soweit möglich, die virtuelle Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed bereit, um Leistung und Betrieb der virtuellen Appliance zu optimieren.

- **Thin Provision** erstellt eine Festplatte im Thin-Format. Die Festplatte vergrößert sich mit anwachsendem Volumen der auf ihr gespeicherten Daten. Wenn Ihr Speichergerät keine Festplatten vom Typ Thick-Provisioning unterstützt oder Sie ungenutzten Speicherplatz auf der virtuellen Log Insight-Appliance einsparen möchten, stellen Sie die virtuelle Appliance mit Festplatten vom Typ Thin-Provisioning bereit.

HINWEIS Das Verkleinern von Festplatten auf der virtuellen Log Insight-Appliance wird nicht unterstützt und kann zu Datenbeschädigung oder -verlust führen.

- 5 (Optional) Stellen Sie auf der Seite „Eigenschaften“ die Netzwerkparameter für die virtuelle Log Insight-Appliance ein.

Wenn Sie keine Netzwerkeinstellungen wie IP-Adresse, DNS-Server und Gateway vornehmen, verwendet Log Insight DHCP, um diese Einstellungen vorzunehmen.



VORSICHT Geben Sie nicht mehr als zwei Domännennamenserver an. Wenn Sie mehr als zwei Domännennamenserver angeben, werden alle konfigurierten Domännennamenserver in der virtuellen Log Insight-Appliance ignoriert.

Trennen Sie Domännennamenserver mit einem Komma.

- 6 (Optional) Stellen Sie auf der Seite „Eigenschaften“ das Root-Kennwort für die virtuelle Log Insight-Appliance ein.
- 7 Folgen Sie den Eingabeaufforderungen, um die Bereitstellung abzuschließen.

Informationen zur Bereitstellung virtueller Appliances finden Sie im *Benutzerhandbuch für die Bereitstellung von vApps und virtuellen Appliances*.

Nach dem Einschalten der virtuellen Appliance beginnt eine Initialisierung. Das Abschließen der Initialisierung kann unter Umständen mehrere Minuten dauern. Am Ende des Vorgangs erfolgt ein Neustart der virtuellen Appliance.

- 8 Gehen Sie zur Registerkarte **Konsole** und überprüfen Sie die IP-Adresse der virtuellen Log Insight-Appliance.

IP-Adresspräfix	Beschreibung
https://	Die DHCP-Konfiguration in der virtuellen Appliance ist korrekt.
http://	Die DHCP-Konfiguration in der virtuellen Appliance ist fehlgeschlagen. - a Schalten Sie die virtuelle Log Insight-Appliance aus. - b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie Einstellungen bearbeiten. - c Legen Sie eine statische IP-Adresse für die virtuelle Appliance fest.

Weiter

- Konfigurieren Sie das Root-Kennwort in der Konsole der virtuellen Appliance, um SSH-Verbindungen zur virtuellen Log Insight-Appliance zu aktivieren. Weitere Informationen finden Sie unter *Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance* im *Log Insight-Administratorhandbuch*.
- Informationen zum Konfigurieren einer eigenständigen Bereitstellung von Log Insight finden Sie unter dem Thema *Konfigurieren einer neuen Bereitstellung von Log Insight* in der Anleitung *Erste Schritte für Log Insight*.

Die Log Insight-Web-Benutzeroberfläche ist über <https://log-insight-host/> verfügbar, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Hinzufügen zu einer vorhandenen Bereitstellung

Nach Bereitstellung und Einrichtung eines eigenständigen Log Insight-Knotens können Sie eine neue Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen Log Insight - Cluster zu bilden.

Log Insight ermöglicht eine horizontale Skalierung durch den Einsatz mehrerer virtueller Appliance-Instanzen. Dies ermöglicht eine lineare Skalierung des Aufnahmedurchsatzes, erhöht die Abfrageleistung und sorgt für Hochverfügbarkeit bei der Aufnahme. Im Cluster-Modus bietet Log Insight Master- und Worker-Knoten. Master- und Worker-Knoten sind für eine Teilmenge von Daten verantwortlich. Master-Knoten können alle Teilmengen von Daten abfragen und die Ergebnisse aggregieren.

WICHTIG Es wird nachdrücklich empfohlen, dass Sie in einem Log Insight-Cluster mindestens drei Knoten konfigurieren, um Aufnahme, Konfiguration und eine hohe Verfügbarkeit des Benutzerspeicherplatzes zu bieten.

Voraussetzungen

- Notieren Sie in vSphere Client die IP-Adresse der virtuellen Log Insight-Worker-Appliance.
- Sie müssen die IP-Adresse oder den Hostnamen der virtuellen Log Insight-Master-Appliance kennen.
- Stellen Sie sicher, dass Sie über ein Administratorkonto auf der virtuellen Log Insight-Master-Appliance verfügen.

- Stellen Sie sicher, dass die Versionen der Log Insight-Master- und Worker-Knoten synchron sind. Fügen Sie einem Log Insight-Master-Knoten einer neueren Version keinen Log Insight-Worker-Knoten einer älteren Version hinzu.
- Sie müssen die Uhrzeit der virtuellen Log Insight Linux Agent-Appliance mit einem NTP-Server synchronisieren. Weitere Informationen finden Sie im Thema *Synchronisieren der Uhrzeit der virtuellen Log Insight-Appliance* im *Log Insight-Administratorhandbuch*.
- Weitere Informationen zu unterstützten Browser-Versionen finden Sie im Abschnitt *Mindestanforderungen* der Anleitung *Erste Schritte für VMware vRealize Log Insight*.

Vorgehensweise

- 1 Verwenden Sie einen unterstützten Browser, um zur Web-Benutzeroberfläche des Log Insight-Workers zu navigieren.

Das URL-Format lautet `https://log_insight-host/`, wobei `log_insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Worker-Appliance ist.

Der Erstkonfigurationsassistent wird geöffnet.
- 2 Klicken Sie auf **Hinzufügen zu einer vorhandenen Bereitstellung**.
- 3 Geben Sie die IP-Adresse oder den Hostnamen des Log Insight-Masters ein und klicken Sie auf **Los**.

Der Worker sendet eine Anfrage an den Log Insight-Master, der vorhandenen Bereitstellung beizutreten.
- 4 Klicken Sie auf den Link **Klicken Sie hier, um auf die Seite „Clusterverwaltung“ zuzugreifen**.
- 5 Melden Sie sich als Administrator an.

Die Cluster-Seite wird geladen.
- 6 Klicken Sie auf **Zulassen**.

Der Worker wird der vorhandenen Bereitstellung hinzugefügt und Log Insight wird als Cluster betrieben.

Weiter

- Stellen Sie, um einen weiteren Worker hinzuzufügen, eine neue Log Insight-Instanz bereit und fügen Sie diese über den Startassistenten dem Cluster hinzu.
- Wiederholen Sie das Verfahren, um mindestens zwei Log Insight-Worker-Knoten hinzuzufügen.

Aktualisieren eines Worker-Knotens in einem Log Insight -Cluster

Worker-Knoten in einem Log Insight-Cluster können aktualisiert werden.

Der Log Insight-Master-Knoten aktualisiert die Worker-Knoten zentral über die Web-Benutzeroberfläche.

WICHTIG Gehen Sie beim Aktualisieren oder Hinzufügen von Log Insight-Cluster-Knoten immer der Reihe nach vor. Vermeiden Sie gleichzeitige Aktualisierungen bzw. Hinzufügungen, da dies zu Konsistenzproblemen führen kann.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der `.pak`-Datei für das Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

- Aktualisieren Sie den Master-Knoten des Log Insight-Clusters. Weitere Informationen hierzu finden Sie unter „[Upgrade von Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche](#)“, auf Seite 12.
- Wenn Sie ein externes Lastenausgleichsmodul verwenden, nehmen Sie den Knoten aus diesem Modul heraus, bevor Sie ihn in den Wartungsmodus versetzen.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Cluster**.
- 3 Suchen Sie in der Tabelle „Worker“ den gewünschten Knoten und klicken Sie auf  und dann auf **Weiter**.

Der Knoten befindet sich jetzt im Wartungsmodus.

HINWEIS Ein Knoten im Wartungsmodus erhält weiterhin Protokolle.

- 4 Klicken Sie auf  und anschließend zur Bestätigung auf **Upgrade des Workers**.

HINWEIS Das Symbol  ist nur für Worker mit älteren Versionen als der Master verfügbar. Das Symbol  wird nicht mehr angezeigt, nachdem der Worker auf die Version des Masters aktualisiert wurde.

Nach dem Upgrade wird der Worker neu gestartet und neu mit dem Cluster verbunden.

Weiter

Aktualisieren Sie die übrigen Worker-Knoten in Ihrem Log Insight-Cluster.

Entfernen eines Worker-Knotens aus einem Log Insight -Cluster

Sie können einen Worker-Knoten aus einem Log Insight-Cluster entfernen und diesen einem anderen Cluster hinzufügen oder eine eigenständige Bereitstellung starten.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Wenn Sie ein externes Lastenausgleichsmodul verwenden, nehmen Sie den Knoten aus diesem Modul heraus, bevor Sie ihn in den Wartungsmodus versetzen.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Cluster**.
- 3 Suchen Sie in der Tabelle „Worker“ den gewünschten Knoten und klicken Sie auf  und dann auf **Weiter**.

Der Knoten befindet sich jetzt im Wartungsmodus.

HINWEIS Ein Knoten im Wartungsmodus erhält weiterhin Protokolle.

- 4 Klicken Sie auf , um den Knoten zu entfernen.

Log Insight entfernt den Knoten aus dem Cluster und sendet eine E-Mail-Benachrichtigung.

Beispiel:

Weiter

Navigieren Sie zur Web-Benutzeroberfläche des entfernten Knotens, um diesen zu konfigurieren. Sie können den Knoten einem anderen bestehenden Log Insight-Cluster hinzufügen oder eine neue eigenständige Bereitstellung starten.

Aktivieren des integrierten Lastenausgleichsmoduls

Sie können das integrierte Lastenausgleichsmodul in einem Log Insight-Cluster aktivieren, um sicherzustellen, dass der eingehende Aufnahmeverkehr von Log Insight akzeptiert wird, selbst wenn einige Log Insight-Knoten nicht verfügbar sein sollten.

Es wird dringend empfohlen, in einer Log Insight-Clusterumgebung den integrierten Lastenausgleichsdienst zu aktivieren.

Dieser stellt sicher, dass der eingehende Aufnahmeverkehr von Log Insight akzeptiert wird, selbst wenn einige Log Insight-Knoten nicht verfügbar sein sollten. Außerdem verteilt der integrierte Lastenausgleichsdienst den eingehenden Datenverkehr gleichmäßig auf alle verfügbaren Log Insight-Knoten. Log Insight-Clients, die sowohl die Web-Benutzeroberfläche als auch die Aufnahme (über Syslog oder die Ingestion-API) verwenden, sollten sich über die IP-Adresse des integrierten Lastenausgleichsdiensts mit Log Insight verbinden.

Für den integrierten Lastenausgleichsdienst müssen alle Log Insight-Knoten im selben Layer-2-Netzwerk liegen, beispielsweise hinter demselben Switch, oder auf sonstige Weise in der Lage sein, ARP-Anforderungen untereinander zu versenden oder zu empfangen. Die IP-Adresse des integrierten Lastenausgleichsdiensts muss so eingerichtet sein, dass jeder Log Insight-Knoten über sie Datenverkehr empfangen kann. Das bedeutet üblicherweise, dass sich die IP-Adresse des integrierten Lastenausgleichsdiensts im selben Subnetz wie die physische Adresse der Log Insight-Knoten befindet. Nach der Konfiguration der IP-Adresse des integrierten Lastenausgleichsdiensts versuchen Sie einen Ping von einem anderen Netzwerk aus, um sicherzugehen, dass sie erreicht werden kann.

Um zukünftige Änderungen und Upgrades möglichst einfach zu gestalten, können Clients auf einen FQDN verweisen, der die IP-Adresse des integrierten Lastenausgleichsdiensts auflöst, anstatt direkt auf die IP-Adresse des integrierten Lastenausgleichsdiensts zu verweisen.

Voraussetzungen

- Konfigurieren Sie mindestens drei Knoten in einem Log Insight-Cluster.
- Überprüfen Sie, dass sich alle Log Insight-Knoten und die angegebene IP-Adresse des integrierten Lastenausgleichsdiensts im selben Netzwerk befinden.
- Die Master- und Worker-Knoten von Log Insight müssen dieselben Zertifikate aufweisen. Andernfalls lehnen die Log Insight-Agents, die für die Verbindung mit SSL konfiguriert sind, die Verbindung ab. Setzen Sie beim Hochladen eines von einer Zertifizierungsstelle signierten Zertifikats auf Master- und Worker-Knoten von Log Insight den allgemeinen Namen während der Zertifikatserstellungsanfrage auf die IP-Adresse des integrierten Lastenausgleichsdiensts. Weitere Informationen hierzu finden Sie unter [„Generieren einer Zertifizierungsanforderung“](#), auf Seite 89.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Cluster**.

- 3 Wählen Sie unter „Konfiguration“ die Option **Integrierten Lastenausgleichsdienst aktivieren** und geben Sie die virtuelle IP-Adresse für den integrierten Lastenausgleich ein.

Richten Sie die Clients so ein, dass diese auf einen vollständig qualifizierten Domännennamen anstatt auf die IP-Adresse des integrierten Lastenausgleichsdiensts verweisen.

- 4 Klicken Sie auf **Speichern**.

Prüfen des Systemzustands der virtuellen Log Insight -Appliance

Sie können die verfügbaren Ressourcen und aktiven Abfragen auf der virtuellen Log Insight-Appliance überprüfen und aktuelle Statistiken über den Betrieb von Log Insight aufrufen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **System-Monitor**.
- 3 Wenn Log Insight als Cluster ausgeführt wird, klicken Sie auf **Ressourcen anzeigen für** und wählen Sie den Knoten aus, den Sie überwachen möchten.
- 4 Klicken Sie auf die Schaltflächen auf der Seite „Systemüberwachung“, um die benötigten Informationen anzuzeigen.

Option	Beschreibung
Ressourcen	Anzeigen von Informationen über CPU, Arbeitsspeicher, IOPS (Lese- und Schreibvorgänge) und Speichernutzung auf der virtuellen Log Insight-Appliance. Die Diagramme auf der rechten Seite zeigen historische Daten der letzten 24 Stunden und werden alle fünf Minuten aktualisiert. Die Diagramme auf der linken Anzeige enthalten Informationen der letzten fünf Minuten und werden alle drei Sekunden aktualisiert.
Aktive Abfragen	Anzeigen von Informationen zu den derzeit in Log Insight aktiven Abfragen.
Statistiken	Anzeigen von Statistiken zu den Protokollaufnahmevergängen und -raten. Um detaillierte Statistiken anzuzeigen, klicken Sie auf Erweiterte Statistik anzeigen .

Weiter

Sie können mit den Informationen der Seite „Systemüberwachung“ Ressourcen auf der virtuellen Log Insight-Appliance verwalten.

Protokollspeicherrichtlinie

Die virtuelle Log Insight-Appliance benötigt mindestens 100 GB Speicher für eingehende Protokolle.

Wenn das Volumen der in Log Insight importierten Protokolle die 100-GB-Grenze erreicht, werden alte Protokollmeldungen automatisch und in regelmäßigen Abständen in der Eingangsreihenfolge stillgelegt. Um alte Meldungen aufzubewahren, können Sie die Archivierungsfunktion von Log Insight aktivieren. Weitere Informationen hierzu finden Sie unter „[Aktivieren oder Deaktivieren der Datenarchivierung in Log Insight](#)“, auf Seite 85.

Von Log Insight gespeicherte Daten sind unveränderbar. Nachdem ein Protokoll importiert wurde, kann dieses erst entfernt werden, wenn es automatisch stillgelegt wird.

Erhöhen der Speicherkapazität der virtuellen Log Insight -Appliance

Sie können die Speicherressourcen, die Log Insight zugewiesen sind, erhöhen, wenn Ihre Nachfrage wächst.

Den Speicherplatz vergrößern Sie, indem Sie der virtuellen Log Insight-Appliance eine neue virtuelle Festplatte hinzufügen. Sie können so viele Festplatten hinzufügen, wie Sie benötigen und wie Ihre Umgebung zulässt.

Voraussetzungen

- Melden Sie sich bei vSphere Client als Benutzer mit Berechtigungen zum Ändern der Hardware der virtuellen Maschinen in Ihrer Umgebung an.
- Fahren Sie die virtuelle Log Insight-Appliance sicher herunter. Weitere Informationen hierzu finden Sie unter „[Ausschalten der virtuellen Log Insight-Appliance](#)“, auf Seite 99.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der vSphere Client-Bestandsliste auf die virtuelle Log Insight-Maschine und wählen Sie **Einstellungen bearbeiten** aus.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **Festplatte**, und klicken Sie auf **Weiter**.

4 Wählen Sie **Neue virtuelle Festplatte erstellen**, und klicken Sie auf **Weiter**.

- a Geben Sie die Festplattenkapazität ein.

Log Insight unterstützt virtuelle Festplatten von bis zu 2 TB. Wenn Sie mehr Kapazität benötigen, fügen Sie mehr als eine virtuelle Festplatte hinzu.

- b Auswählen eines Festplattenformats.

Option	Beschreibung
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird bei Erstellung der virtuellen Festplatte zugewiesen. Die Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt nach dem ersten Schreibvorgang von der virtuellen Appliance gelöscht.
Thick-Provision Eager-Zeroed	Erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen. Erstellen Sie, soweit möglich, die virtuelle Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed, um Leistung und Betrieb der virtuellen Appliance zu optimieren.
Thin Provision	Erstellt eine Festplatte im Thin-Format. Verwenden Sie dieses Format, um Speicherplatz zu sparen.

- c Zum Auswählen eines Datenspeichers navigieren Sie zum Speicherort des Datenspeichers und klicken auf **Weiter**.

5 Akzeptieren Sie den Standardknoten des virtuellen Geräts und klicken Sie auf **Weiter**.

6 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn Sie die virtuelle Log Insight-Appliance hochfahren, erkennt die virtuelle Maschine die neue Festplatte und fügt sie dem Datenvolumen hinzu.



VORSICHT Nachdem Sie eine Festplatte zur virtuellen Appliance hinzugefügt haben, können Sie sie nicht mehr auf sichere Weise entfernen. Das Entfernen von Festplatten von der virtuellen Log Insight-Appliance kann zu einem vollständigen Datenverlust führen.

Überwachen von Protokollereignisse sendenden Hosts

Sie können eine Liste mit allen Hosts und Geräten anzeigen, die Protokollereignisse an Log Insight senden, um diese zu überwachen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.

- 2 Klicken Sie unter „Verwaltung“ auf **Hosts**.

HINWEIS Wenn Sie einen vCenter Server zum Senden von Ereignissen und Warnungen konfiguriert haben, die einzelnen ESXi-Hosts jedoch nicht zum Senden von Protokollen konfiguriert haben, werden in der Liste „Hostname“ nicht nur die vCenter Server-Hosts, sondern auch die einzelnen ESXi-Hosts als Quelle aufgelistet.

Überwachen des Status von Log Insight Windows und Linux Agents

Sie können den Status der Log Insight Windows und Linux Agents überwachen und aktuelle Statistiken über deren Betrieb anzeigen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Agents**.

Weiter

Anhand der Informationen auf der Seite „Agents“ können Sie den Betrieb der installierten Log Insight Windows und Linux Agents überwachen.

Verwalten von Benutzerkonten in Log Insight

Administratoren können Benutzerkonten anlegen, um Benutzern den Zugriff auf die Log Insight-Web-Benutzeroberfläche zu ermöglichen.

Nur Benutzer mit der Berechtigung **Admin bearbeiten** können alle Benutzerkonten erstellen und bearbeiten.

Benutzer, die nicht über die Berechtigung **Admin bearbeiten** verfügen, können nur ihre eigenen Konten – beispielsweise das E-Mail- oder Kontokennwort – ändern.

Benutzerverwaltung – Übersicht

Systemadministratoren nutzen eine Kombination aus Benutzeranmeldungen, einer rollenbasierten Zugriffssteuerung, Berechtigungen und Datensätzen zur Verwaltung von Log Insight-Benutzern. Mit der rollenbasierten Zugriffssteuerung können Administratoren Benutzer und die Aufgaben, die diese wahrnehmen, verwalten.

Bei den Rollen handelt es sich um Berechtigungssätze, die zur Durchführung bestimmter Aufgaben erforderlich sind. Systemadministratoren definieren Rollen als Teil der Definition von Sicherheitsrichtlinien und weisen die Rollen dann den Benutzern zu. Zum Ändern der Berechtigungen und der Aufgaben, die einer bestimmten Aufgabe zugewiesen sind, aktualisiert der Systemadministrator die Rolleneinstellungen. Die aktualisierten Einstellungen treten für alle Benutzer, die der Rolle zugewiesen sind, in Kraft.

- Um einem Benutzer die Durchführung einer Aufgabe zu gestatten, weist der Systemadministrator dem Benutzer die Rolle zu.
- Um einen Benutzer von der Durchführung einer Aufgabe abzuhalten, hebt der Systemadministrator die Zuweisung der Rolle zum Benutzer wieder auf.

Die Verwaltung des Zugriffs, der Rollen und Berechtigungen für jeden Benutzer basiert auf dem jeweiligen Benutzeranmeldungs-konto. Jedem Benutzer können verschiedene Rollen und Berechtigungen zugewiesen werden.

Benutzern, die bestimmte Objekte nicht sehen bzw. nicht darauf zugreifen können, oder die bestimmte Operationen nicht durchführen können, wurden die entsprechenden Berechtigungen dafür nicht zugewiesen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung können Systemadministratoren den Benutzerzugriff auf Log Insight sowie Aufgaben steuern, die Benutzer nach erfolgreicher Anmeldung durchführen können. Um die rollenbasierte Zugriffssteuerung zu implementieren, ordnen Systemadministratoren Berechtigungen und Rollen mit oder aus Benutzeranmeldekonto zu oder heben diese auf.

Benutzer	Systemadministratoren können den Zugriff und die Aktionen aller Benutzer steuern, indem sie für das Anmeldekonto des Benutzers Berechtigungen und Rollen gewähren oder diese aufheben.
Berechtigungen	Mit Berechtigungen werden die zulässigen Aktionen in Log Insight gesteuert. Berechtigungen werden auf bestimmte Verwaltungs- oder Benutzeraufgaben in Log Insight angewendet. Beispiel: Sie können die Berechtigung Admin anzeigen gewähren, um einem Benutzer zu erlauben, auf die administrativen Log Insight-Einstellungen zuzugreifen.
Datensätze	Datensätze bestehen aus einer Gruppe von Filtern. Sie können Datensätze verwenden, um Benutzern Zugriff auf bestimmten Inhalt zu ermöglichen, indem ein Datensatz mit einer Rolle verknüpft wird.
Rollen	Rollen sind Sammlungen aus Berechtigungen und Datensätzen, die mit Benutzern verbunden werden können. Mit Rollen können alle für eine auszuführende Aufgabe erforderlichen Berechtigungen auf bequeme Weise gebündelt werden. Ein Benutzer kann mehreren Rollen zugewiesen werden.

Erstellen eines neuen Benutzerkontos in Log Insight

Benutzer, denen die Rolle „Super Admin“ zugewiesen wird, können Benutzerkonten anlegen, um so den Zugang zur Log Insight-Web-Benutzeroberfläche zu gewähren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffssteuerung**.
- 3 Klicken Sie auf **Benutzer und Gruppen**.
- 4 Klicken Sie auf **Neuer Benutzer**.
- 5 Wählen Sie im Dropdown-Menü **Authentifizierung** die Option **Standard (integriert)** aus.
- 6 Geben Sie einen Benutzernamen und eine E-Mail-Adresse ein.

Die E-Mail-Adresse ist optional.

- 7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von Log Insight verwenden.
Nur Admin anzeigen	Admin anzeigen-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von Log Insight zugreifen, können Log Insight verwalten und die Konten aller Benutzer verwalten.

- 8 Kopieren Sie das Kennwort aus dem Textfeld **Kennwort** und stellen Sie es dem Benutzer zur Verfügung.
- 9 Klicken Sie auf **Speichern**.

Hinzufügen eines Active Directory-Benutzers zu Log Insight

Sie können Active Directory-Benutzern (AD) erlauben, sich mit ihren Domänen-Anmeldedaten bei Log Insight anzumelden.

Wenn Sie die AD-Unterstützung in Log Insight aktivieren, konfigurieren Sie einen Domänennamen und geben Sie einen Bindungsbenutzer an, der zur Domäne gehört. Log Insight verwendet den Bindungsbenutzer, um die Verbindung zur AD-Domäne und das Vorhandensein von AD-Benutzern und -Gruppen zu überprüfen.

AD-Benutzer, die Sie Log Insight hinzufügen, müssen entweder der Domäne des Bindungsbenutzers oder einer Domäne, die der Domäne des Bindungsbenutzers vertraut, angehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass die AD-Unterstützung konfiguriert ist. Weitere Informationen hierzu finden Sie unter „[Aktivieren der Benutzerauthentifizierung über Active Directory](#)“, auf Seite 86.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.
- 3 Klicken Sie auf **Neuer Benutzer**.
- 4 Wählen Sie im Dropdown-Menü **Authentifizierungsmethode** die Option **Active Directory**.

Der von Ihnen bei der Konfiguration der AD-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt. Wenn Sie Benutzer der Standarddomäne hinzufügen, dürfen Sie den Domänennamen nicht ändern.

- 5 (Optional) Wenn Sie einen Benutzer aus einer Domäne, die der Standarddomäne vertraut, hinzufügen möchten, geben Sie den Namen der vertrauenden Domäne im Textfeld **Domäne** ein.
- 6 Geben Sie den Namen eines Domänenbenutzers ein.
- 7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von Log Insight verwenden.
Nur Admin anzeigen	Admin anzeigen-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von Log Insight zugreifen, können Log Insight verwalten und die Konten aller Benutzer verwalten.

- 8 Klicken Sie auf **Speichern**.

Log Insight prüft, ob der Benutzer in der von Ihnen angegebenen Domäne oder deren vertrauenswürdigen Domänen vorhanden ist. Wenn der Benutzer nicht vorhanden ist, werden Sie durch ein Dialogfeld darauf hingewiesen, dass Log Insight den Benutzer nicht bestätigen kann. Sie können den Benutzer ohne Bestätigung speichern oder den Vorgang abbrechen und den Benutzernamen korrigieren.

Von Ihnen hinzugefügte AD-Benutzer können sich mit ihren Domänen-Anmeldedaten bei Log Insight anmelden.

Hinzufügen einer Active Directory-Gruppe zu Log Insight

Anstatt einzelne Domänenbenutzer hinzuzufügen, können Sie Domänengruppen hinzufügen, um den Benutzern die Anmeldung bei Log Insight zu gestatten.

Wenn Sie die AD-Unterstützung in Log Insight aktivieren, konfigurieren Sie einen Domänennamen und geben Sie einen Bindungsbenutzer an, der zur Domäne gehört. Log Insight verwendet den Bindungsbenutzer, um die Verbindung zur AD-Domäne und das Vorhandensein von AD-Benutzern und -Gruppen zu überprüfen.

Die AD-Gruppen, die Sie Log Insight hinzufügen, müssen entweder der Domäne des Bindungsbenutzers oder einer Domäne, der die Domäne des Bindungsbenutzers vertraut, angehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass die AD-Unterstützung konfiguriert ist. Weitere Informationen hierzu finden Sie unter „[Aktivieren der Benutzerauthentifizierung über Active Directory](#)“, auf Seite 86.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.
- 3 Klicken Sie auf **Benutzer und Gruppen**.
- 4 Klicken Sie unter „Active Directory-Gruppen“ auf **Neue Gruppe**.

Der von Ihnen bei der Konfiguration der AD-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt. Wenn Sie Gruppen zur Standarddomäne hinzufügen, dürfen Sie den Domänennamen nicht ändern.

- 5 (Optional) Wenn Sie eine Gruppe aus einer Domäne, die der Standarddomäne vertraut, hinzufügen möchten, geben Sie den Namen der vertrauenden Domäne in das Textfeld **Domäne** ein.
- 6 Geben Sie den Namen der AD-Gruppe ein, die Sie hinzufügen möchten.
- 7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von Log Insight verwenden.
Nur Admin anzeigen	Admin anzeigen-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von Log Insight zugreifen, können Log Insight verwalten und die Konten aller Benutzer verwalten.

- 8 Klicken Sie auf **Speichern**.

Log Insight verifiziert, ob die AD-Gruppe in der Domäne, die Sie angegeben haben, oder in einer vertrauenswürdigen Domäne vorhanden ist. Wenn die Gruppe nicht gefunden wird, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie darüber informiert werden, dass Log Insight diese Gruppe nicht verifizieren kann. Sie können die Gruppe ohne Verifizierung speichern oder den Vorgang abbrechen und den Gruppennamen korrigieren.

Benutzer, die zu der AD-Gruppe gehören, die Sie hinzugefügt haben, können sich über ihr Domänenkonto bei Log Insight anmelden. Sie verfügen dann über dieselbe Berechtigungsstufe wie die Gruppe, der sie angehören.

Definieren eines Datensatzes

Sie können einen Datensatz definieren, um Benutzerzugriff auf bestimmte Inhalte zu gewährleisten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.
- 3 Klicken Sie auf **Datensätze**.
- 4 Klicken Sie auf **Neuer Datensatz**.
- 5 Klicken Sie auf **Filter hinzufügen**.
- 6 Verwenden Sie das erste Dropdown-Menü, um ein beliebiges innerhalb von Log Insight definiertes Feld zu verwenden.

Beispiel: **hostname**.

Die Liste enthält alle definierten Felder, die statisch verfügbar sind, Inhaltspaketen und in benutzerdefiniertem Inhalt.

HINWEIS Numerische Felder enthalten zusätzliche Operatoren, die in Zeichenfolgenfeldern nicht vorkommen: =, >, <, >= und <=. Diese Operatoren führen numerische Vergleiche aus. Durch ihre Verwendung können andere Ergebnisse als bei der Verwendung von Zeichenfolgenoperatoren erzielt werden. Beispiel: Der Filter **response_time = 02** ergibt als Treffer ein Ereignis, das ein Feld **response_time** mit einem Wert von 2 enthält. Der Filter **response_time enthält 02** ergibt nicht denselben Treffer.

- 7 Verwenden Sie das zweite Dropdown-Menü, um den Vorgang auszuwählen, der auf das im ersten Dropdown-Menü ausgewählte Feld angewendet werden soll.
- Wählen Sie zum Beispiel **enthält**. Der Filter **enthält** gleicht vollständige Token ab: Wenn Sie z. B. den Suchbegriff „err“ eingeben, werden keine Übereinstimmungen mit error ausgegeben.
- 8 Geben Sie im Textfeld rechts neben dem Dropdown-Menü für den Filter den Wert ein, den Sie als Filter verwenden möchten.

Sie können mehrere Werte verwenden. Der Operator zwischen diesen Werten ist ODER.

HINWEIS Das Textfeld ist nicht verfügbar, wenn Sie im zweiten Dropdown-Menü den Operator **ist vorhanden** auswählen.

- 9 (Optional) Klicken Sie auf **Filter hinzufügen**, um weitere Filter hinzuzufügen.
- 10 Klicken Sie auf **Speichern**.

Weiter

Ordnen Sie einer Benutzerrolle einen Datensatz zu. Weitere Informationen hierzu finden Sie unter „[Erstellen und Ändern von Rollen](#)“, auf Seite 27.

Erstellen und Ändern von Rollen

Sie können benutzerdefinierte Rollen erstellen oder vordefinierte Rollen ändern, um den Benutzern die Durchführung bestimmter Aufgaben sowie den Zugriff auf bestimmte Inhalte zu gestatten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.

- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.
- 3 Klicken Sie auf **Rollen**.
- 4 Klicken Sie auf **Neue Rolle** oder auf , um eine vorhandene Rolle zu bearbeiten.
Sie müssen zunächst die Rollen „Super Admin“ und „Benutzer“ klonen, bevor Sie sie bearbeiten können.
- 5 Ändern Sie die Textfelder **Name** und **Beschreibung**.
- 6 Wählen Sie eine oder mehrere Berechtigung(en) aus der Liste „Berechtigungen“ aus.

Option	Beschreibung
Admin bearbeiten	Damit können Admin-Informationen und -Einstellungen bearbeitet werden
Admin anzeigen	Damit können Admin-Informationen und -Einstellungen angezeigt werden
Freigegebene bearbeiten	Damit können freigegebene Inhalte bearbeitet werden
Analytics	Damit kann die Interaktive Analyse verwendet werden
Dashboard	Damit können Dashboards angezeigt werden

- 7 (Optional) Wählen Sie rechts aus der Liste **Datensätze** einen Datensatz aus, welcher der Benutzerrolle zugewiesen werden soll.
- 8 Klicken Sie auf **Speichern**.

Löschen eines Benutzerkontos aus Log Insight

Benutzerkonten können über die Benutzeroberfläche für Administratoren von Log Insight gelöscht werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.
- 3 Klicken Sie auf **Benutzer und Gruppen**.
- 4 Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen, der gelöscht werden soll.
- 5 Klicken Sie auf das Symbol **Löschen** .

Übersicht über den Log Insight Windows Agent

Der Log Insight Windows Agent erfasst Ereignisse aus Windows-Ereigniskanälen und Protokolldateien und leitet sie an den Log Insight-Server weiter.

Ein Windows-Ereigniskanal ist ein Pool zur Erfassung verwandter Ereignisse in einem Windows-System. Standardmäßig erfasst der Log Insight Windows Agent Ereignisse aus den Kanälen Anwendung, System und Sicherheit.

In Windows-Systemen können Anwendungen Protokolldaten in Text-Flatfiles im Dateisystem speichern. Der Log Insight Windows Agent kann Verzeichnisse überwachen und Ereignisse aus Textprotokoll-Flatfiles erfassen.

Der Log Insight Windows Agent weist eine Beschränkung von 64 KB pro Anforderung an den Log Insight-Server auf.

Der Log Insight Windows Agent wird als Windows-Dienst ausgeführt und startet sofort nach der Installation. Während und nach der Installation können Sie die folgenden Optionen für den Log Insight Windows Agent einstellen:

- Wählen Sie den Log Insight-Zielserver aus, an den der Log Insight Windows Agent die Ereignisse weiterleitet.
- Wählen Sie das Kommunikationsprotokoll und den Port des Log Insight Windows Agent aus.
- Fügen Sie zusätzliche Windows-Ereigniskanäle hinzu, aus denen der Log Insight Windows Agent Ereignisse erfassen soll.
- Wählen Sie die Windows-Verzeichnisse aus, die überwacht werden sollen, und fügen Sie zu erfassende Flatfile-Protokolldateien hinzu.

Der Log Insight Windows Agent erfordert Windows Vista oder höher bzw. Windows Server 2008 oder höher.

Zum Herunterladen der .msi-Datei für Log Insight Windows Agent navigieren Sie zur Verwaltungsseite der Web-Benutzeroberfläche von Log Insight und klicken Sie im Abschnitt „Verwaltung“ auf **Agents** und anschließend auf den Link zum Herunterladen des Log Insight Windows Agent.

Installieren des Log Insight Windows Agent mit Standardkonfiguration

Installieren Sie den Log Insight Windows Agent mit Standardkonfiguration unter Verwendung des GUI-Assistenten.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der Log Insight Windows Agent .msi-Datei verfügen. Um die Log Insight Windows Agent .msi-Datei herunterzuladen, navigieren Sie zur Seite **Verwaltung** der Log Insight-Web-Benutzeroberfläche, klicken Sie im Verwaltungsabschnitt auf **Agents** und dann auf den Link „Log Insight Windows Agent herunterladen“.
- Stellen Sie sicher, dass Sie über Berechtigungen zum Ausführen von Installationen und zum Starten von Diensten auf dem Windows-Computer verfügen.

Vorgehensweise

- 1 Protokoll Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installieren möchten.
- 2 Wechseln Sie zu dem Verzeichnis, in dem die Log Insight Windows Agent .msi-Datei gespeichert ist.
- 3 Doppelklicken Sie im Log Insight Windows Agent auf die .msi-Datei, akzeptieren Sie die Bedingungen des Lizenzvertrags und klicken Sie auf **Weiter**.
- 4 Geben Sie die IP-Adresse oder den Hostnamen des Log Insight-Servers ein und klicken Sie auf **Installieren**.

Der Assistent installiert den Log Insight Windows Agent als einen automatischen Windows-Dienst unter dem LocalSystem-Dienstkonto.

- 5 Klicken Sie auf **Beenden**.

Weiter

Konfigurieren Sie den Log Insight Windows Agent, indem Sie die Datei `liagent.ini` bearbeiten. Weitere Informationen finden Sie im Thema über die Log Insight Windows Agent-Konfiguration im Log Insight-Administratorhandbuch.

Installieren des Log Insight Windows Agent mit Parametern

Installieren Sie den Log Insight Windows Agent unter Verwendung der Windows-Befehlszeile und geben Sie Konfigurationsparameter an.

Informationen zu MSI-Befehlszeilenoptionen finden Sie auf der Website der MSDN-Bibliothek (Microsoft Developer Network), wenn Sie nach MSI-Befehlszeilenoptionen suchen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der Log Insight Windows Agent .msi-Datei verfügen. Um die Log Insight Windows Agent .msi-Datei herunterzuladen, navigieren Sie zur Seite **Verwaltung** der Log Insight-Web-Benutzeroberfläche, klicken Sie im Verwaltungsabschnitt auf **Agents** und dann auf den Link „Log Insight Windows Agent herunterladen“.
- Stellen Sie sicher, dass Sie über Berechtigungen zum Ausführen von Installationen und zum Starten von Diensten auf dem Windows-Computer verfügen.
- Wenn Sie die Option für die unbeaufsichtigte Installation `/quiet` oder `/qn` verwenden, stellen Sie sicher, dass Sie die Installation als Administrator ausführen. Wenn Sie die unbeaufsichtigte Installation als Nicht-Administrator ausführen, werden bei der Installation keine Administratorberechtigungen angefordert und die Installation schlägt fehl. Verwenden Sie die Protokollierungsoptionen und Parameter `/lxv* file_name` für Diagnosezwecke.

Vorgehensweise

- 1 Protokoll Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installieren möchten.
- 2 Öffnen Sie ein Eingabeaufforderungsfenster.
- 3 Wechseln Sie zu dem Verzeichnis, in dem die Log Insight Windows Agent .msi-Datei gespeichert ist.
- 4 Führen Sie den folgenden Befehl aus, um die Installation zu starten:

Drive: `\path-to-msi_file>VMware-Log-Insight-Agent-*.msi` und ersetzen Sie * mit Ihrer Version und Build-Nummer.

- 5 (Optional) Geben Sie ein Benutzerdienstkonto an, unter dem der Log Insight Windows Agent-Dienst ausgeführt wird.

Drive: `\path-to-msi_file>VMware-Log-Insight-Agent-*.msi SERVICEACCOUNT=domain\user SERVICE-PASSWORD=user_password`

HINWEIS Das im Parameter SERVICEACCOUNT angegebene Konto muss über die Berechtigung **Anmelden als Dienst** verfügen und vollständigen Schreibzugriff auf das Verzeichnis %ProgramData%\VMware\Log Insight Agent haben. Wenn das angegebene Konto nicht vorhanden ist, wird es erstellt. Der Benutzername darf 20 Zeichen nicht überschreiten. Wenn Sie keinen SERVICEACCOUNT-Parameter angeben, wird der Log Insight Windows Agent-Dienst unter dem LocalSystem-Dienstkonto installiert.

- 6 (Optional) Geben Sie den Log Insight-Server, den Port und das Protokoll an.

Parameter	Beschreibung
SERVERHOST	Die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance.
SERVERPROTO	Das Protokoll, das der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die möglichen Werte lauten <code>cfapi</code> und <code>syslog</code> . VMware empfiehlt die Verwendung der <code>cfapi</code> -Standardeinstellung.
SERVERPORT	Die Portnummer richtet sich nach dem Wert von <code>SERVERPROTO</code> . Der Standardwert für <code>SERVERPORT</code> lautet 9000, der dem Standard- <code>SERVERPROTO=cfapi</code> entspricht. Verwenden Sie <code>SERVERPORT=514</code> für <code>SERVERPROTO=syslog</code> .

Die Befehlszeilenparameter entsprechen `hostname`, `proto` und `port` im Abschnitt `[server]` der Datei `liagent.ini`.

- 7 Drücken Sie die Eingabetaste.

Der Befehl installiert den Log Insight Windows Agent als Windows-Dienst. Der Log Insight Windows Agent-Dienst wird automatisch beim Starten des Windows-Computers gestartet.

Weiter

Stellen Sie sicher, dass die von Ihnen festgelegten Befehlszeilenparameter in der Datei `liagent.ini` ordnungsgemäß angewendet werden. Siehe „[Konfigurieren des Log Insight Windows Agent nach der Installation](#)“, auf Seite 31.

Konfigurieren des Log Insight Windows Agent nach der Installation

Der Log Insight Windows Agent kann nach der Installation konfiguriert werden. In der Datei `liagent.ini` können Sie Log Insight Windows Agent so konfigurieren, dass Ereignisse an den gewünschten Log Insight-Server gesendet werden, das Kommunikationsprotokoll und die entsprechenden Port festlegen, Windows-Ereigniskanäle hinzufügen und die Flatfile-Protokollierung konfigurieren.

Standardkonfiguration des Log Insight Windows Agent

Nach der Installation enthält die `liagent.ini`-Datei vorkonfigurierte Standardeinstellungen für den Log Insight Windows Agent.

liagent.ini-Standardkonfiguration

```
[server]
hostname=LOGINSIGHT
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
;hostname=LOGINSIGHT

; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 514
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9543
```

```

;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is yes.
;ssl=yes

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

[storage]
;max_disk_buffer – max disk usage limit (data + logs) in MB:
; 100 – 2000 MB, default 200
;max_disk_buffer=200

[logging]
;debug_level – the level of debug messages to enable:
; 0 – no debug messages
; 1 – trace essential debug messages
; 2 – verbose debug messages (will have negative impact on performace)
;debug_level=0

[winlog|Application]
channel=Application

[winlog|Security]
channel=Security

[winlog|System]
channel=System

```

Parameter	Wert	Beschreibung
proto	cfapi	Das Protokoll, das der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die möglichen Werte lauten cfapi und syslog. VMware empfiehlt die Verwendung der cfapi-Standardeinstellung.
hostname	LOGINSIGHT	Die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance.
port	9543	Der Kommunikationsport, den der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die Standardwerte lauten 9543 für cfapi mit SSL-Aktivierung, 9000 für cfapi mit SSL-Deaktivierung und 514 für syslog.
ssl	yes	Aktiviert oder deaktiviert SSL. Der Standardwert lautet „ja“. Nur auf cfapi anwendbar.
max_disk_buffer	200	Die maximale Festplattengröße in MB, die der Log Insight Windows Agent zum Puffern von Ereignissen und seinen eigenen Protokollen verwendet.

Parameter	Wert	Beschreibung
debug_level	0	Legt die Protokolldateiebene fest. Weitere Informationen hierzu finden Sie unter „ Festlegen der Protokolldateiebene in den Log Insight Agents “, auf Seite 54.
channel	Application, Security, System	Die Standardkanäle für das Windows-Ereignisprotokoll, die der Log Insight Windows Agent erfasst. Siehe „ Erfassen von Ereignissen aus Windows-Ereigniskanälen “, auf Seite 34.

Festlegen des Log Insight -Zielservers

Sie können den Log Insight-Zielserver festlegen oder ändern, der dem Log Insight Windows Agent Ereignisse sendet, wenn Sie die Werte während der Installation nicht festgelegt haben.

Voraussetzungen

- Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.
- Wenn Sie über einen Log Insight-Cluster mit integriertem Lastenausgleich verfügen, finden Sie unter „[Aktivieren des integrierten Lastenausgleichsmoduls](#)“, auf Seite 18 Informationen zu den spezifischen Anforderungen für benutzerdefinierte SSL-Zertifikate.

Vorgehensweise

- 1 Navigieren Sie zum Programmdatenordner von Log Insight Windows Agent.
%ProgramData%\VMware\Log Insight Agent
- 2 Öffnen Sie die Datei liagent.ini in einem beliebigen Texteditor.
- 3 Ändern Sie die folgenden Parameter und legen Sie die Werte für Ihre Umgebung fest.

Parameter	Beschreibung
proto	Das Protokoll, das der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die möglichen Werte lauten <code>cfapi</code> und <code>syslog</code> . VMware empfiehlt die Verwendung der <code>cfapi</code> -Standardeinstellung.
hostname	Die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance.
port	Der Kommunikationsport, den der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die Standardwerte lauten 9543 für <code>cfapi</code> mit SSL-Aktivierung, 9000 für <code>cfapi</code> mit SSL-Deaktivierung und 514 für <code>syslog</code> .
ssl	Aktiviert oder deaktiviert SSL. Der Standardwert lautet „ja“. Nur auf <code>cfapi</code> anwendbar.
reconnect	Das Zeitintervall in Minuten, in dem der erneute Verbindungsaufbau zum Server erzwungen wird. Der Standardwert lautet 30.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
;hostname=LOGINSIGHT

; Set protocol to use:
; cfapi - Log Insight REST API
```

```

; syslog – Syslog protocol
; If omitted the default value is cfapi
;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 514
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9543

;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is yes.
;ssl=yes

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

```

- 4 Speichern und schließen Sie die Datei liagent.ini.

Beispiel: Konfiguration

Im folgenden Konfigurationsbeispiel wird ein Log Insight-Zielserver festgelegt.

```

[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes

```

Weiter

Sie können weitere SSL-Optionen für den Log Insight Windows Agent festlegen. Weitere Informationen hierzu finden Sie unter [„Konfigurieren der SSL-Verbindung zwischen dem Log Insight-Server und den Log Insight Agents“](#), auf Seite 91.

Erfassen von Ereignissen aus Windows-Ereigniskanälen

Sie können einen Windows-Ereigniskanal zur Log Insight Windows Agent-Konfiguration hinzufügen. Der Log Insight Windows Agent erfasst die Ereignisse und sendet sie an den Log Insight-Server.

Voraussetzungen

Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zum Programmdatenordner von Log Insight Windows Agent.
`%ProgramData%\VMware\Log Insight Agent`
- 2 Öffnen Sie die Datei liagent.ini in einem beliebigen Texteditor.

- 3 Fügen Sie die folgenden Parameter hinzu und legen Sie die Werte für Ihre Umgebung fest.

Parameter	Beschreibung
[winlog section_name]	Ein eindeutiger Name für den Konfigurationsabschnitt.
channel	Der vollständige Name des Ereigniskanals, wie in der Ereignisanzeige der integrierten Windows-Anwendung, angezeigt. Um den richtigen Kanalnamen zu kopieren, klicken Sie in der Ereignisanzeige mit der rechten Maustaste auf einen Kanal, wählen Sie Eigenschaften aus und kopieren Sie die Inhalte des Felds Vollständiger Name.
enabled	Ein optionaler Parameter zum Aktivieren oder Deaktivieren des Konfigurationsabschnitts. Die möglichen Werte lauten yes oder no . Der Standardwert lautet yes .
tags	Ein optionaler Parameter zum Hinzufügen von benutzerdefinierten Tags zu den Feldern der erfassten Ereignisse. Definieren Sie Tags mit der JSON-Notation. Tagnamen können Buchstaben, Zahlen und Unterstriche enthalten. Ein Tagname darf nur mit einem Buchstaben oder einem Unterstrich beginnen und darf nicht mehr als 64 Zeichen enthalten. Die Groß- und Kleinschreibung wird bei Tagnamen nicht berücksichtigt. Wenn Sie zum Beispiel <code>tags= {"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" }</code> verwenden, wird <code>Tag_Name1</code> als Duplikat ignoriert. Sie können „event_type“ und „timestamp“ nicht als Tagnamen verwenden. Alle Duplikate innerhalb derselben Deklaration werden ignoriert.
whitelist, blacklist	Optionale Parameter zum expliziten Einbeziehen oder Ausschließen von Protokollereignissen.
exclude_fields	(Optional) Ein Parameter zum Ausschließen einzelner Felder aus der Erfassung. Sie können mehrere Werte als eine durch Semikolons getrennte Liste eingeben. Beispiel: <code>exclude_fields=EventId; ProviderName</code>

```
[winlog|section_name]
channel=event_channel_name
enabled=yes_or_no
tags={"tag_name1" : "Tag value 1", "tag_name2" : "tag value 2" }
```

- 4 Speichern und schließen Sie die Datei `liagent.ini`.

Beispiel: Konfigurationen

Beachten Sie die folgenden [winlog]-Konfigurationsbeispiele.

```
[winlog|Events_Firewall ]
channel=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
enabled=no

[winlog|custom]
channel=Custom
tags={"ChannelDescription": "Events testing channel"}
```

Einrichten der Windows-Ereigniskanal-Filterung

Sie können Filter für Windows-Ereigniskanäle einrichten, um Protokollereignisse explizit aufzunehmen bzw. auszuschließen.

Zur Auswertung eines Filterausdrucks verwenden Sie die Parameter `whitelist` und `blacklist`. Der Filterausdruck ist ein boolescher Ausdruck, der aus Windows-Ereignisfeldern und -Operanden besteht.

- `whitelist` erfasst nur Protokollereignisse, für welche die Auswertung des Filterausdrucks ungleich null ist. Wenn Sie `whitelist`, auslassen, ist der Wert eine implizierte 1.
- `blacklist` schließt Protokollereignisse aus, bei denen die Auswertung des Filterausdrucks ungleich null ist. Der Standardwert ist 0.

Eine umfassende Liste der Windows-Ereignisfelder und -Operanden finden Sie unter „[Ereignisfelder und Operanden](#)“, auf Seite 37.

Voraussetzungen

Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zum Programmdatenordner von Log Insight Windows Agent.
`%ProgramData%\VMware\Log Insight Agent`
- 2 Öffnen Sie die Datei `liagent.ini` in einem beliebigen Texteditor.
- 3 Fügen Sie den Parameter `whitelist` oder `blacklist` im Abschnitt `[winlog]` hinzu.
 Beispiel:

```
[winlog|unique_section_name]
channel = event_channel_name
blacklist = filter_expression
```
- 4 Erstellen Sie einen Filterausdruck aus Windows-Ereignisfeldern und -Operanden.
 Beispiel:
`whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO`
- 5 Speichern und schließen Sie die Datei `liagent.ini`.

Beispiel: Filterkonfigurationen

Sie können den Agent beispielsweise so konfigurieren, dass nur Fehlerereignisse erfasst werden.

```
[winlog|Security-Error]
channel = Security
whitelist = Level == WINLOG_LEVEL_CRITICAL or Level == WINLOG_LEVEL_ERROR
```

Sie können den Agent beispielsweise so konfigurieren, dass nur VMware Network-Ereignisse aus dem Anwendungskanal erfasst werden.

```
[winlog|VMwareNetwork]
channel = Application
whitelist = ProviderName == "VMnetAdapter" or ProviderName == "VMnetBridge" or ProviderName == "VMnetDHCP"
```

Sie können den Agent beispielsweise so konfigurieren, dass mit Ausnahme bestimmter Ereignisse alle Ereignisse aus dem Sicherheitskanal erfasst werden.

```
[winlog|Security-Verbose]
channel = Security
blacklist = EventID == 4688 or EventID == 5447
```

Ereignisfelder und Operanden

Erstellen Sie Filterausdrücke mithilfe der Windows-Ereignisfelder und -Operanden.

Filtern von Ausdrucksoperanden

Operator	Beschreibung
==, !=	gleich und ungleich. Sowohl mit Zahlen- als auch mit Zeichenfolgenfeldern verwenden.
>=, >, <, <=	größer oder gleich, größer als, kleiner als, kleiner oder gleich. Nur mit Zahlenfeldern verwenden.
&, , ^, ~	Bitweise AND, OR, XOR und ergänzende Operanden. Nur mit Zahlenfeldern verwenden.
and, or	Logisches AND und OR. Für den Aufbau komplexer Ausdrücke durch Kombination von Einzelausdrücken.
not	Unär logischer NOT-Operand. Für die Umkehr des Werts eines Ausdrucks.
()	Verwenden Sie Klammern in einem logischen Ausdruck, um die Auswertungsreihenfolge zu ändern.

Windows-Ereignisfelder

Sie können die folgenden Windows-Ereignisfelder in einem Filterausdruck verwenden:

Feldname	Feldtyp
Hostname	String
Text	String
ProviderName	String
EventSourceName	String
EventID	numeric
EventRecordID	numeric
Channel	String
UserID	String
Level	numeric Sie können die folgenden vordefinierten Konstanten verwenden. ■ WINLOG_LEVEL_SUCCESS = 0 ■ WINLOG_LEVEL_CRITICAL = 1 ■ WINLOG_LEVEL_ERROR = 2 ■ WINLOG_LEVEL_WARNING = 3 ■ WINLOG_LEVEL_INFO = 4 ■ WINLOG_LEVEL_VERBOSE = 5
Task	numeric
OpCode	numeric
Keywords	numeric Sie können die folgenden vordefinierten Bitmasken verwenden: ■ WINLOG_KEYWORD_RESPONSETIME = 0x0001000000000000; ■ WINLOG_KEYWORD_WDICONTEXT = 0x0002000000000000; ■ WINLOG_KEYWORD_WDIDIAGNOSTIC = 0x0004000000000000; ■ WINLOG_KEYWORD_SQM = 0x0008000000000000; ■ WINLOG_KEYWORD_AUDITFAILURE = 0x0010000000000000; ■ WINLOG_KEYWORD_AUDITSUCCESS = 0x0020000000000000; ■ WINLOG_KEYWORD_CORRELATIONHINT = 0x0040000000000000; ■ WINLOG_KEYWORD_CLASSIC = 0x0080000000000000;

Beispiele

Erfassen aller kritischen Ereignisse sowie Fehler- und Warnereignisse

```
[winlog|app]
channel = Application
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

Erfassen nur von Auditfehler-Ereignissen über den Sicherheitskanal

```
[winlog|security]
channel = Security
whitelist = Keywords & WINLOG_KEYWORD_AUDITFAILURE
```

Erfassen von Ereignissen aus einer Protokolldatei

Der Log Insight Windows Agent kann so konfiguriert werden, dass er Ereignisse aus einer oder mehreren Protokolldateien erfasst.

Voraussetzungen

Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zum Programmdatenordner von Log Insight Windows Agent.
%ProgramData%\VMware\Log Insight Agent
- 2 Öffnen Sie die Datei liagent.ini in einem beliebigen Texteditor.
- 3 Fügen Sie Konfigurationsparameter hinzu und legen Sie die Werte für Ihre Umgebung fest.

Parameter	Beschreibung
[filelog section_name]	Ein eindeutiger Name für den Konfigurationsabschnitt.
directory	Der vollständige Pfad zum Protokolldateiverzeichnis.
include	(Optional) Der Name eines Dateinamens oder einer Dateimaske (Glob-Muster) für die Datenerfassung. Sie können Werte als eine durch Semikolons getrennte Liste eingeben. Der Standardwert lautet *. Das heißt, dass alle Dateien berücksichtigt werden. Bei dem Parameter muss die Groß-/Kleinschreibung beachtet werden. HINWEIS .zip- und .gz-Dateien werden standardmäßig nicht erfasst. Wenn Sie .zip- und .gz-Dateien erfassen möchten, fügen Sie sie unter Verwendung des Parameters include hinzu. WICHTIG Verwenden Sie bei der Erfassung einer rotierten Protokolldatei die Parameter include und exclude, um ein Glob-Muster anzugeben, das der primären und der rotierten Datei entspricht. Wenn das Glob-Muster nur der primären Protokolldatei entspricht, verpassen die Log Insight Agents möglicherweise Ereignisse während der Rotation. Die Log Insight Agents legen die richtige Reihenfolge der rotierten Dateien automatisch fest und senden Ereignisse an den Log Insight-Server in der richtigen Reihenfolge. Wenn es sich beispielsweise bei Ihrer primären Protokolldatei um myapp.log und bei den rotierten Protokollen um myapp.log.1, myapp.log.2 usw. handelt, können Sie das folgende include-Muster verwenden: include= myapp.log;myapp.log.*
exclude	(Optional) Ein Dateiname oder eine Dateimaske (Glob-Muster) zum Ausschließen aus der Erfassung. Sie können Werte als eine durch Semikolons getrennte Liste eingeben. Der Standardwert ist leer. Das heißt, dass keine Datei ausgeschlossen wird.

Parameter	Beschreibung
event_marker	(Optional) Ein regulärer Ausdruck, der den Start eines Ereignisses in der Protokolldatei angibt. Wird dieser Ausdruck weggelassen, wird standardmäßig ein Zeilenumbruch ausgeführt. Die von Ihnen eingegebenen Ausdrücke müssen die Perl-Syntax für reguläre Ausdrücke verwenden.
enabled	(Optional) Ein Parameter zum Aktivieren oder Deaktivieren des Konfigurationsabschnitts. Die möglichen Werte lauten yes oder no. Der Standardwert lautet yes.
charset	(Optional) Die Zeichenkodierung der Protokolldateien, die der Agent überwacht. Die möglichen Werte lauten UTF-8, UTF-16LE und UTF-16BE. Der Standardwert lautet UTF-8.
tags	(Optional) Ein Parameter zum Hinzufügen von benutzerdefinierten Tags zu den Feldern der erfassten Ereignisse. Definieren Sie Tags mit der JSON-Notation. Tagnamen können Buchstaben, Zahlen und Unterstriche enthalten. Ein Tagname darf nur mit einem Buchstaben oder einem Unterstrich beginnen und darf nicht mehr als 64 Zeichen enthalten. Die Groß- und Kleinschreibung wird bei Tagnamen nicht berücksichtigt. Wenn Sie zum Beispiel tags= {"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" } verwenden, wird Tag_Name1 als Duplikat ignoriert. Sie können „event_type“ und „timestamp“ nicht als Tagnamen verwenden. Alle Duplikate innerhalb derselben Deklaration werden ignoriert. Tags können das APP-NAME-Feld überschreiben, wenn das Ziel ein Syslog-Server ist. Beispiel: tags={"appname":"VROPS"}.
exclude_fields	(Optional) Ein Parameter zum Ausschließen einzelner Felder aus der Erfassung. Sie können mehrere Werte als eine durch Semikolons getrennte Liste eingeben. Beispiel: exclude_fields=hostname; filepath

```
[filelog|section_name]
directory=path_to_log_directory
include=glob_pattern
```

Beispiel: Konfigurationen

```
[filelog|vCenterMain]
directory=C:\ProgramData\VMware\VMware VirtualCenter\Logs
include=vpxd-*.log
exclude=vpxd-alert-*.log;vpxd-profiler-*.log
event_marker=^\d{4}-\d{2}-\d{2}[A-Z]\d{2}:\d{2}:\d{2}\.\d{3}

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
tags={"Provider" : "Apache"}

[filelog|MSSQL]
directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log
charset=UTF-16LE
event_marker=^[^\s]
```

Zentrale Konfiguration von Log Insight Windows Agents

Sie können mehrere Log Insight Windows Agents über die Web-Benutzeroberfläche von Log Insight konfigurieren.

Jeder Log Insight Windows Agent weist eine lokale Konfiguration und eine serverseitige Konfiguration auf. Die lokale Konfiguration wird in einer `liagent.ini`-Datei auf dem Computer gespeichert, auf dem der Log Insight Windows Agent installiert ist. Die serverseitige Konfiguration kann auf der Seite **Verwaltung > Agents** der Web-Benutzeroberfläche geöffnet und bearbeitet werden. Die Konfiguration jedes Log Insight Windows Agent setzt sich aus Abschnitten und Schlüsseln zusammen. Schlüssel haben konfigurierbare Werte.

Der Log Insight Windows Agents fragt den Log Insight-Server in regelmäßigen Abständen ab und empfängt die serverseitige Konfiguration. Die serverseitige und die lokale Konfiguration werden zusammengeführt und das Ergebnis stellt eine effektive Konfiguration dar. Jeder Log Insight Windows Agent verwendet die effektive Konfiguration als seine Betriebskonfiguration. Konfigurationen werden abschnittsweise und Schlüssel für Schlüssel zusammengeführt. Die Werte in der serverseitigen Konfiguration überschreiben die Werte in der lokalen Konfiguration. Die Zusammenführungsregeln lauten wie folgt:

- Wenn ein Abschnitt nur in der lokalen oder nur in der serverseitigen Konfiguration vorhanden ist, werden dieser Abschnitt und der entsprechende Inhalt Teil der effektiven Konfiguration.
- Wenn ein Abschnitt sowohl in der lokalen als auch in der serverseitigen Konfiguration vorhanden ist, werden die Schlüssel im Abschnitt gemäß der folgenden Regeln zusammengeführt:
 - Wenn ein Schlüssel nur in der lokalen oder nur in der serverseitigen Konfiguration vorhanden ist, werden der Schlüssel und die entsprechenden Werte Teil dieses Abschnitts in der effektiven Konfiguration.
 - Wenn ein Schlüssel sowohl in der lokalen als auch in der serverseitigen Konfiguration vorhanden ist, wird der Schlüssel Teil dieses Abschnitts in der effektiven Konfiguration und der Wert in der serverseitigen Konfiguration wird verwendet.

Ein Log Insight-Administrator kann die zentrale Konfiguration auf alle Log Insight Windows Agents unter Verwendung der Web-Benutzeroberfläche von Log Insight anwenden. Navigieren Sie zur Seite „Verwaltung“ und klicken Sie im Abschnitt „Verwaltung“ auf **Agents**. Geben Sie die Konfigurationseinstellungen im Feld **Agent-Konfiguration** ein und klicken Sie auf **Konfiguration für alle Agents speichern**. Die Konfiguration wird beim nächsten Abrufzyklus auf alle verbundenen Agents angewendet.

HINWEIS Die zentrale Konfiguration kann nur auf Log Insight Windows Agents angewendet werden, die das cfapi-Protokoll verwenden.

Weitere Informationen hierzu finden Sie unter [„Konfigurieren des Log Insight Windows Agent nach der Installation“](#), auf Seite 31.

Exemplarische Konfigurationszusammenführung

Exemplarische Zusammenführung einer lokalen und einer serverseitigen Log Insight Windows Agent-Konfiguration.

Lokale Konfiguration

Sie können die folgende lokale Log Insight Windows Agent-Konfiguration haben.

```
[server]
proto=cfapi
hostname=HOST
port=9000

[winlog|Application]
channel=Application
```

```
[winlog|Security]
channel=Security
```

```
[winlog|System]
channel=System
```

```
[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^\d{1,3}\.){3}\d{1,3} - -
```

Serverseitige Konfiguration

Sie können die Seite **Verwaltung > Agents** der Web-Benutzeroberfläche zur Anwendung einer zentralen Konfiguration für alle Agents verwenden. Beispiel: Sie können Erfassungskanäle ausschließen und hinzufügen und die Standard-Neuverbindungseinstellung ändern.

```
[server]
reconnect=20
```

```
[winlog|Security]
channel=Security
enabled=no
```

```
[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational
```

Effektive Konfiguration

Die effektive Konfiguration ist das Ergebnis der Zusammenführung der lokalen mit der serverseitigen Konfiguration. Der Log Insight Windows Agent ist auf Folgendes konfiguriert:

- Neuverbindung mit dem Log Insight-Server alle 20 Minuten
- mit der Erfassung von Anwendungs- und Systemereigniskanälen fortfahren
- die Erfassung des Sicherheitseigniskanals stoppen
- mit der Erfassung des Microsoft-Windows-DeviceSetupManager-Ereigniskanals/operativen Ereigniskanals beginnen
- die Erfassung von ApacheAccessLogs fortsetzen

```
[server]
proto=cfapi
hostname=HOST
port=9000
reconnect=20
```

```
[winlog|Application]
channel=Application
```

```
[winlog|Security]
channel=Security
enabled=no
```

```
[winlog|System]
```

```
channel=System
```

```
[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational
```

```
[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(\d{1,3}\.){3}\d{1,3} - -
```

Weiterleiten von Ereignissen an den Log Insight Windows Agent

Sie können Ereignisse von Windows-Systemen an ein System weiterleiten, auf dem der Log Insight Windows Agent ausgeführt wird.

Sie können die Windows-Ereignisweiterleitung nutzen, um Ereignisse von mehreren Windows-Computern an einen Computer zu senden, auf dem Log Insight Windows Agent installiert ist. Dann können Sie den Log Insight Windows Agent so konfigurieren, dass alle weitergeleiteten Ereignisse erfasst und an einen Log Insight-Server gesendet werden.

Machen Sie sich mit der Windows-Ereignisweiterleitung vertraut. Siehe <http://technet.microsoft.com/en-us/library/cc748890.aspx> und [http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx).

Voraussetzungen

Weitere Informationen hierzu finden Sie unter „Erfassen von Ereignissen aus Windows-Ereigniskanälen“, auf Seite 34.

Vorgehensweise

- 1 Fügen Sie der Log Insight Windows Agent-Konfiguration eine neue Seite hinzu, um Ereignisse aus dem Windows-Ereigniskanal, der weitergeleitete Ereignisse empfängt, zu erfassen.

Der Standard-Kanalname lautet ForwardedEvents.

- 2 Richten Sie die Windows-Ereignisweiterleitung ein.

Weiter

Navigieren Sie zur Log Insight-Web-Benutzeroberfläche und stellen Sie sicher, dass weitergeleitete Ereignisse eintreffen.

Bereitstellen des Log Insight Windows Agent auf mehreren Computern

Der Log Insight Windows Agent kann auf mehreren Computern in der Windows-Domäne bereitgestellt werden.

Vorbereiten der Bereitstellung der .msi-Datei für den Log Insight Windows Agent .

Zum Festlegen von Installationsparametern, die während der Bereitstellung verwendet werden, erstellen Sie eine .mst-Umwandlungsdatei. Sie können den Log Insight Windows Agent so konfigurieren, dass Ereignisse an einen Log Insight-Server Ihrer Wahl gesendet werden. Darüber hinaus können Sie das Kommunikationsprotokoll, den Port und das Benutzerkonto für die Installation und den Beginn des Log Insight Agent-Diensts festlegen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der Log Insight Windows Agent .msi-Datei verfügen. Um die Log Insight Windows Agent .msi-Datei herunterzuladen, navigieren Sie zur Seite **Verwaltung** der Log Insight-Web-Benutzeroberfläche, klicken Sie im Verwaltungsabschnitt auf **Agents** und dann auf den Link „Log Insight Windows Agent herunterladen“.
- Laden Sie den Orca-Datenbankeditor herunter und installieren Sie ihn. Siehe <http://support.microsoft.com/kb/255905>.

Vorgehensweise

- 1 Öffnen Sie die Log Insight Windows Agent .msi-Datei im Orca-Editor, und klicken Sie auf **Umwandeln > Neu umwandeln**.
- 2 Bearbeiten Sie die Tabelle „Eigenschaft“ und fügen Sie die nötigen Parameter und Werte für die benutzerdefinierte Installation oder das benutzerdefinierte Upgrade hinzu.

Parameter	Beschreibung
SERVERHOST	Die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance.
SERVERPROTO	Das Protokoll, das der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die möglichen Werte lauten <code>cfapi</code> und <code>syslog</code> . VMware empfiehlt die Verwendung der <code>cfapi</code> -Standardeinstellung.
SERVERPORT	Der Kommunikationsport, den der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die Standardwerte lauten 9543 für <code>cfapi</code> mit SSL-Aktivierung, 9000 für <code>cfapi</code> mit SSL-Deaktivierung und 514 für <code>syslog</code> .
SERVICEACCOUNT	Das Benutzerdienstkonto, unter dem der Log Insight Windows Agent-Dienst ausgeführt wird. HINWEIS Das im Parameter <code>SERVICEACCOUNT</code> angegebene Konto muss über die Berechtigung Anmelden als Dienst und über Schreibzugriff für das Verzeichnis <code>%ProgramData%\VMware\Log Insight Agent</code> verfügen, damit das Installationsprogramm ordnungsgemäß ausgeführt wird. Wenn Sie keinen <code>SERVICEACCOUNT</code> -Parameter angeben, wird der Log Insight Windows Agent-Dienst im LocalSystem-Dienstkonto installiert.
SERVICEPASSWORD	Das Kennwort des Benutzerdienstkontos.

- 3 Klicken Sie auf **Umwandeln > Umwandlung generieren** und speichern Sie die .mst-Datei.

Weiter

Verwenden Sie die .msi-Datei und die .mst-Datei für die Log Insight Windows Agent-Bereitstellung.

Massenbereitstellung des Log Insight Windows Agent

Die Massenbereitstellung des Log Insight Windows Agent ist auf Zielcomputern in der Windows-Domäne möglich.

Machen Sie sich mit den Verfahren in <http://support.microsoft.com/kb/887405> und <http://support.microsoft.com/kb/816102> vertraut.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Administratorkonto bzw. ein Konto mit Administratorrechten im Domänencontroller verfügen.
- Vergewissern Sie sich, dass Sie über eine Kopie der Log Insight Windows Agent .msi-Datei verfügen. Um die Log Insight Windows Agent .msi-Datei herunterzuladen, navigieren Sie zur Seite **Verwaltung** der Log Insight-Web-Benutzeroberfläche, klicken Sie im Verwaltungsabschnitt auf **Agents** und dann auf den Link „Log Insight Windows Agent herunterladen“.

Vorgehensweise

- 1 Melden Sie sich beim Domänencontroller (DC) als Administrator bzw. Benutzer mit Administratorrechten an.
- 2 Definieren Sie einen Bereitstellungspunkt und kopieren Sie die .msi-Datei für den Log Insight Windows Agent an den Bereitstellungspunkt.
- 3 Öffnen Sie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC) und erstellen Sie ein Grupperichtlinienobjekt (Group Policy Object, GPO) zur Bereitstellung der .msi-Datei für den Log Insight Windows Agent.
- 4 Bearbeiten Sie das GPO für die Softwarebereitstellung und weisen Sie ein Paket zu.
- 5 (Optional) Wenn Sie vor der Bereitstellung eine .mst-Datei erstellt haben, bearbeiten Sie ein GPO zur Bereitstellung des .msi-Pakets mithilfe der fortgeschrittenen Methode. Wählen Sie die .mst-Konfigurationsdatei auf der Registerkarte **Änderungen** des Fensters GPO-Eigenschaften.
- 6 (Optional) Um den Log Insight Windows Agent zu aktualisieren, kopieren Sie die .msi-Upgradedatei an den Bereitstellungspunkt und gehen Sie zur Registerkarte **Upgrade** des Fensters GPO-Properties. Fügen Sie die anfangs installierte Version der .msi-Datei in den Abschnitt „Pakete, die dieses Paket aktualisiert“ ein.
- 7 Stellen Sie den Log Insight Windows Agent für bestimmte Sicherheitsgruppen bereit, die die Domänenbenutzer umfassen.
- 8 Schließen Sie alle Fenster der GPMC- und GPM-Editoren im DC und starten Sie die Clientcomputer zweimal neu.
- 9 Überprüfen Sie, ob Log Insight Windows Agent auf den Clientcomputern als lokaler Dienst installiert wurde.

Wenn Sie die Parameter SERVICEACCOUNT und SERVICEPASSWORD für die Massenbereitstellung mithilfe einer .mst-Datei konfiguriert haben, müssen Sie sicherstellen, dass Log Insight Windows Agent auf den Clientcomputern im angegebenen Benutzerkonto installiert ist.

Weiter

Wenn die Massenbereitstellung des Log Insight Windows Agent nicht erfolgreich war, siehe „[Die Massenbereitstellung des Log Insight Windows Agent ist nicht erfolgreich](#)“, auf Seite 58.

Deinstallieren des Log Insight Windows Agent

Sie können den Log Insight Windows Agent deinstallieren.

Voraussetzungen

Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zu **Systemsteuerung > Programme und Funktionen**.
- 2 Wählen Sie den Log Insight Windows Agent von VMware vRealize aus und klicken Sie auf **Deinstallieren**.

Das Deinstallationsprogramm beendet den VMware vRealize Log Insight Windows Agent-Dienst und entfernt die entsprechenden Dateien aus dem System.

Erstellen eines Support-Pakets für den Log Insight Windows Agent

Falls der Log Insight Windows Agent aufgrund eines Problems nicht wie erwartet funktioniert, können Sie eine Kopie der Protokoll- und Konfigurationsdateien an die VMware Support-Dienste senden.

Vorgehensweise

- 1 Melden Sie sich bei dem Zielcomputer an, auf dem der Log Insight Windows Agent installiert ist.
- 2 Klicken Sie auf die Windows-Schaltfläche **Start** und wählen Sie **VMware > Log Insight Agent - Support-Paket erfassen** aus.
- 3 (Optional) Wenn die Verknüpfung nicht verfügbar ist, navigieren Sie zum Installationsverzeichnis von Log Insight Windows Agent und doppelklicken Sie auf `loginsight-agent-support.exe`.

HINWEIS Das Standardinstallationsverzeichnis lautet `C:\Programme (x86)\VMware\Log Insight Agent`.

Das Paket wird generiert und als ZIP-Datei in **Eigene Dokumente** gespeichert.

Weiter

Leiten Sie das Support-Paket wie verlangt an die VMware Support-Dienste weiter.

Übersicht über den Log Insight Linux Agent

Der Log Insight Linux Agent erfasst Ereignisse aus Protokolldateien auf Linux-Computern und leitet sie an den Log Insight-Server weiter.

In einem Linux-System können Anwendungen Daten in Flat-Textdateien im Dateisystem speichern. Der Log Insight Linux Agent kann Verzeichnisse überwachen und Ereignisse aus Flat-Textprotokolldateien erfassen.

Der Log Insight Linux Agent wird als Daemon ausgeführt und startet sofort nach der Installation. Nach der Installation können Sie die folgenden Optionen konfigurieren:

- Wählen Sie den Log Insight-Zielserver aus, an den der Log Insight Linux Agent Ereignisse weiterleitet.

- Konfigurieren Sie, welche Verzeichnisse der Log Insight Linux Agent überwacht. Standardmäßig ist der Log Insight Linux Agent so konfiguriert, dass er Meldungen und Syslog-Dateien aus dem Verzeichnis `/var/log` erfasst.

```
[filelog|messages]
directory=/var/log
include=messages;messages.?
```

```
[filelog|syslog]
directory=/var/log
include=syslog;syslog.?
```

Der Log Insight Linux Agent unterstützt die folgenden Verteilungen und Versionen.

- RHEL 5 Update 10, RHEL 6 Update 5
- SLES 11 SP3
- Ubuntu 10.04 LTS, 12.04 LTS und 14.04 LTS

Der Log Insight Linux Agent schreibt seine eigenen Betriebsprotokolldateien nach `/var/log/loginsight-agent/liagent_*.log`. Die Protokolldateien rotieren, wenn Log Insight Linux Agent neu gestartet wird und wenn sie eine Größe von 10 MB erreicht haben. Es können Protokolldateien in einem Umfang von max. 50 MB gespeichert werden.

Navigieren Sie zum Herunterladen des Log Insight Linux Agent-Pakets zur Seite „Verwaltung“ der Log Insight-Web-Benutzeroberfläche im Abschnitt „Verwaltung“. Klicken Sie dort auf **Agents** und dann auf die dem Paket entsprechende Verknüpfung.

Installieren oder Aktualisieren des Log Insight Linux Agent -RPM-Pakets

Installieren Sie das Log Insight Linux Agent-RPM-Paket, indem Sie das Systemterminal oder die GUI verwenden.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Der Log Insight Linux Agent benötigt zur ordnungsgemäßen Ausführung Zugriff auf Syslog und Netzwerkdienste. Installieren und führen Sie Log Insight Linux Agent auf den Ausführungsebenen 3 und 5 aus. Wenn der Log Insight Linux Agent auf anderen Ausführungsebenen betrieben werden soll, konfigurieren Sie das System entsprechend.

Vorgehensweise

- 1 Öffnen Sie eine Konsole und führen Sie den Befehl `rpm -i package_name` aus, um den Log Insight Linux Agent zu installieren. Ersetzen Sie *package_name* durch die gewünschte Version. Beispiel:

```
rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

HINWEIS Um den Log Insight-Zielservers während der Installation festzulegen, führen Sie den folgenden Befehl aus, wobei Sie *hostname* durch die IP-Adresse oder den Hostnamen des Log Insight-Servers ersetzen.

```
sudo SERVERHOST=hostname rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

- 2 (Optional) Um den Log Insight Linux Agent zu aktualisieren, führen Sie den folgenden Befehl aus.

```
rpm -Uvh VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

HINWEIS Sie können andere RPM-Befehle wie `-h`, `--hash`, `--version`, `--allfiles` usw. während der Installation, Aktualisierung oder Deinstallation des Log Insight Linux Agent-RPM-Pakets ausführen, diese werden jedoch nicht offiziell unterstützt.

- 3 (Optional) Um den Log Insight Linux Agent als **Nicht-Root**-Benutzer auszuführen, führen Sie den folgenden Befehl aus.

```
sudo LIAGENTUSER=liagent rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

Wenn der angegebene Benutzer nicht vorhanden ist, erstellt der Log Insight Linux Agent das Benutzerkonto während der Installation. Das erstellte Konto wird nach der Deinstallation nicht gelöscht. Wenn Sie den Log Insight Linux Agent mit dem Parameter `LIAGENTUSER=non_root_user` installieren und eine Aktualisierung mit `LIAGENTUSER=non_root_user2` durchführen, tritt ein Konflikt auf und Warnmeldungen werden angezeigt, weil der `non_root_user2`-Benutzer nicht über die Berechtigungen des `non_root_user`-Benutzers verfügt.

- 4 (Optional) Sie können den Log Insight Linux Agent mit der GUI installieren oder aktualisieren. Doppelklicken Sie auf die gewünschte Version des RPM-Pakets.

HINWEIS Upgrades von älteren Versionen des Log Insight Linux Agent von 2.5 TP1, 2.5 TP2 oder 2.5 TP3 auf neuere Versionen werden nicht unterstützt. Sie müssen die älteren RPM-Pakete deinstallieren.

- 5 (Optional) Überprüfen der installierten Version durch Ausführen von `rpm -qa | grep Log-Insight-Agent`

Installieren oder Aktualisieren des DEB-Pakets für den Log Insight Linux Agent

Installieren Sie das DEB-Paket für den Log Insight Linux Agent über das Systemterminal.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Der Log Insight Linux Agent benötigt für den Betrieb Zugriff auf Syslog und die Netzwerkdienste. Standardmäßig wird Log Insight Linux Agent auf den Ausführungsebenen 2, 3, 4 und 5 ausgeführt und auf den Ausführungsebenen 0, 1 und 6 angehalten.

Vorgehensweise

- 1 Öffnen Sie eine Konsole und führen Sie den Befehl `dpkg -i package_name` aus, um den Log Insight Linux Agent zu installieren oder zu aktualisieren. Ersetzen Sie `package_name` durch die entsprechende Version. Beispiel:

```
dpkg -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.deb
```

Um den Log Insight-Zielservers während der Installation festzulegen, führen Sie den folgenden Befehl aus, wobei Sie `hostname` durch die IP-Adresse oder den Hostnamen des Log Insight-Servers ersetzen.

```
sudo SERVERHOST=hostname dpkg -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.deb
```

- 2 (Optional) Um den Log Insight Linux Agent als **Nicht-Root**-Benutzer auszuführen, verwenden Sie folgenden Befehl.

```
sudo LIAGENTUSER=liagent dpkg -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.deb
```

Wenn der angegebene Benutzer nicht existiert, erstellt der Log Insight Linux Agent das entsprechende Benutzerkonto während der Installation. Das erstellte Konto wird nach der Deinstallation nicht gelöscht. Wenn Sie den Log Insight Linux Agent mit dem Parameter `LIAGENTUSER=non_root_user` installieren und ein Upgrade mit `LIAGENTUSER=non_root_user2` versuchen, entsteht ein Konflikt. Sie erhalten Warnmeldungen, weil der Benutzer `non_root_user2` nicht über dieselben Berechtigungen verfügt wie der Benutzer `non_root_user`.

- 3 (Optional) Überprüfen Sie die installierte Version durch Ausführen von `dpkg -l | grep -i VMware-Log-Insight-Agent`.

HINWEIS Upgrades aus älteren Versionen des Log Insight Linux Agent (2.5 TP1, 2.5 TP2 oder 2.5 TP3) auf neuere Versionen werden nicht unterstützt. Ältere DEB-Pakete müssen deinstalliert werden.

Installieren des .bin-Pakets für den Log Insight Linux Agent

Installieren Sie das Binärpaket für den Log Insight Linux Agent über das Systemterminal.

Ein Upgrade des BIN-Pakets wird offiziell nicht unterstützt. Wenn Sie bereits einen Log Insight Linux Agent installiert haben und dieser ein BIN-Paket nutzt, deinstallieren Sie es manuell, bevor Sie die neue Version installieren. Erstellen Sie vor der Deinstallation eine Sicherungskopie der Datei `liagent.ini` unter `/var/lib/loginsight-agent`, um die lokale Konfiguration beizubehalten. Weitere Informationen hierzu finden Sie unter „[Deinstallieren des Log Insight Linux Agent-BIN-Pakets](#)“, auf Seite 53.

Voraussetzungen

- Laden Sie das .bin-Paket für den Log Insight Linux Agent herunter und kopieren Sie es auf den Linux-Zielcomputer.
- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Der Log Insight Linux Agent benötigt für den Betrieb Zugriff auf Syslog und die Netzwerkdienste.

Vorgehensweise

- 1 Öffnen Sie eine Konsole und führen Sie folgenden Befehl aus, um die .bin-Datei in eine ausführbare Datei umzuwandeln: Ersetzen Sie *filename-version* durch die entsprechende Version.

```
chmod +x filename-version.bin
```

- 2 Installieren Sie den Agent, indem Sie den folgenden Befehl ausführen. Ersetzen Sie *filename-version* durch die entsprechende Version.

```
./filename-version.bin
```

HINWEIS Um den Log Insight-Zielserver während der Installation festzulegen, führen Sie den folgenden Befehl aus, wobei Sie *hostname* durch die IP-Adresse oder den Hostnamen des Log Insight-Servers ersetzen.

```
sudo SERVERHOST=hostname ./filename-version.bin
```

- 3 (Optional) Um den Log Insight Linux Agent als **Nicht-Root**-Benutzer auszuführen, verwenden Sie folgenden Befehl.

```
sudo LIAGENTUSER=liagent ./filename-version.bin
```

Wenn der angegebene Benutzer nicht existiert, erstellt der Log Insight Linux Agent das entsprechende Benutzerkonto während der Installation. Das erstellte Konto wird nach der Deinstallation nicht gelöscht. Wenn Sie den Log Insight Linux Agent mit dem Parameter `LIAGENTUSER=non_root_user` installieren und ein Upgrade mit `LIAGENTUSER=non_root_user2` versuchen, entsteht ein Konflikt. Sie erhalten Warnmeldungen, weil der Benutzer `non_root_user2` nicht über dieselben Berechtigungen verfügt wie der Benutzer `non_root_user`.

Konfigurieren des Log Insight Linux Agent

Nachdem Sie Log Insight Linux Agent installiert haben, können Sie ihn konfigurieren. Die Datei `li-agent.ini` ist unter `/var/lib/loginsight-agent/` gespeichert. Bearbeiten Sie die Datei, um Log Insight Linux Agent so zu konfigurieren, dass Ereignisse an einen Log Insight-Server Ihrer Wahl gesendet werden. Legen Sie das Kommunikationsprotokoll und den Kommunikations-Port fest und konfigurieren Sie eine Flat-Datei-Protokollsammlung.

Festlegen des Log Insight-Zielservers

Sie können den Log Insight-Zielserver, an den der Log Insight Linux Agent Ereignisse sendet, festlegen oder ändern.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich bei dem Linux-Computer an, auf dem Sie Log Insight Linux Agent installiert haben. Öffnen Sie eine Konsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass VMware Log Insight Linux Agent installiert ist und ausgeführt wird.
- Wenn Sie über einen Log Insight-Cluster mit integriertem Lastenausgleich verfügen, finden Sie unter „[Aktivieren des integrierten Lastenausgleichsmoduls](#)“, auf Seite 18 Informationen zu den spezifischen Anforderungen für benutzerdefinierte SSL-Zertifikate.

Vorgehensweise

- 1 Öffnen Sie die Datei `/var/lib/loginsight-agent/liagent.ini` in einem beliebigen Texteditor.
- 2 Ändern Sie die folgenden Parameter und legen Sie die Werte für Ihre Umgebung fest.

Parameter	Beschreibung
proto	Das Protokoll, das der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die möglichen Werte lauten <code>cfapi</code> und <code>syslog</code> . VMware empfiehlt die Verwendung der <code>cfapi</code> -Standardeinstellung.
hostname	Die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance.
port	Der Kommunikationsport, den der Agent zum Senden von Ereignissen an den Log Insight-Server verwendet. Die Standardwerte lauten 9543 für <code>cfapi</code> mit SSL-Aktivierung, 9000 für <code>cfapi</code> mit SSL-Deaktivierung und 514 für <code>syslog</code> .

Parameter	Beschreibung
ssl	Aktiviert oder deaktiviert SSL. Der Standardwert lautet „Ja“. Nur auf cfapi anwendbar.
reconnect	Das Zeitintervall in Minuten, in dem der erneute Verbindungsaufbau zum Server erzwungen wird. Der Standardwert lautet 30.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
;hostname=LOGINSIGHT

; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 514
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9543

;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is yes.
;ssl=yes

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

- 3 Speichern und schließen Sie die Datei liagent.ini.

Beispiel: Konfiguration

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes
```

Weiter

Sie können weitere SSL-Optionen für den Log Insight Linux Agent festlegen. Weitere Informationen hierzu finden Sie unter [„Konfigurieren der SSL-Verbindung zwischen dem Log Insight-Server und den Log Insight Agents“](#), auf Seite 91.

Erfassen von Ereignissen aus einer Protokolldatei

Der Log Insight Linux Agent kann so konfiguriert werden, dass er Ereignisse aus einer oder mehreren Protokolldateien erfasst.

HINWEIS Standardmäßig erfasst der Log Insight Linux Agent auch verborgene Dateien wie VIM, CVS, SVN, GIT usw. Wenn diese verborgenen Dateien vom Log Insight Linux Agent nicht erfasst werden sollen, müssen Sie sie manuell ausschließen: **exclude=^\.***.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie **sudo**, um Konsolenbefehle auszuführen.
- Melden Sie sich auf dem Linux-Computer an, auf dem Sie den Log Insight Linux Agent installiert haben, öffnen Sie eine Konsole und führen Sie **pgrep liagent** aus, um sicherzustellen, dass der VMware vRealize Log Insight Linux Agent installiert ist und ausgeführt wird.

Vorgehensweise

- 1 Öffnen Sie die Datei `/var/lib/loginsight-agent/liagent.ini` in einem beliebigen Texteditor.
- 2 Fügen Sie Konfigurationsparameter hinzu und legen Sie die Werte für Ihre Umgebung fest.

Parameter	Beschreibung
[filelog section_name]	Ein eindeutiger Name für den Konfigurationsabschnitt.
directory	Der vollständige Pfad zum Protokolldateiverzeichnis.
include	(Optional) Der Name eines Dateinamens oder einer Dateimaske (Glob-Muster) für die Datenerfassung. Sie können Werte als eine durch Semikolons getrennte Liste eingeben. Der Standardwert lautet <code>*</code>. Das heißt, dass alle Dateien berücksichtigt werden. Bei dem Parameter muss die Groß-/Kleinschreibung beachtet werden. HINWEIS <code>.zip</code>- und <code>.gz</code>-Dateien werden standardmäßig nicht erfasst. Wenn Sie <code>.zip</code>- und <code>.gz</code>-Dateien erfassen möchten, fügen Sie sie unter Verwendung des Parameters <code>include</code> hinzu. WICHTIG Verwenden Sie bei der Erfassung einer rotierten Protokolldatei die Parameter <code>include</code> und <code>exclude</code>, um ein Glob-Muster anzugeben, das der primären und der rotierten Datei entspricht. Wenn das Glob-Muster nur der primären Protokolldatei entspricht, verpassen die Log Insight Agents möglicherweise Ereignisse während der Rotation. Die Log Insight Agents legen die richtige Reihenfolge der rotierten Dateien automatisch fest und senden Ereignisse an den Log Insight-Server in der richtigen Reihenfolge. Wenn es sich beispielsweise bei Ihrer primären Protokolldatei um <code>myapp.log</code> und bei den rotierten Protokollen um <code>myapp.log.1</code>, <code>myapp.log.2</code> usw. handelt, können Sie das folgende <code>include</code>-Muster verwenden: <code>include= myapp.log;myapp.log.*</code>
exclude	(Optional) Ein Dateiname oder eine Dateimaske (Glob-Muster) zum Ausschließen aus der Erfassung. Sie können Werte als eine durch Semikolons getrennte Liste eingeben. Der Standardwert ist leer. Das heißt, dass keine Datei ausgeschlossen wird.
event_marker	(Optional) Ein regulärer Ausdruck, der den Start eines Ereignisses in der Protokolldatei angibt. Wird dieser Ausdruck weggelassen, wird standardmäßig ein Zeilenumbruch ausgeführt. Die von Ihnen eingegebenen Ausdrücke müssen die Perl-Syntax für reguläre Ausdrücke verwenden.
enabled	(Optional) Ein Parameter zum Aktivieren oder Deaktivieren des Konfigurationsabschnitts. Die möglichen Werte lauten <code>yes</code> oder <code>no</code>. Der Standardwert lautet <code>yes</code>.
charset	(Optional) Die Zeichenkodierung der Protokolldateien, die der Agent überwacht. Die möglichen Werte lauten <code>UTF-8</code>, <code>UTF-16LE</code> und <code>UTF-16BE</code>. Der Standardwert lautet <code>UTF-8</code>.

Parameter	Beschreibung
tags	(Optional) Ein Parameter zum Hinzufügen von benutzerdefinierten Tags zu den Feldern der erfassten Ereignisse. Definieren Sie Tags mit der JSON-Notation. Tagnamen können Buchstaben, Zahlen und Unterstriche enthalten. Ein Tagname darf nur mit einem Buchstaben oder einem Unterstrich beginnen und darf nicht mehr als 64 Zeichen enthalten. Die Groß- und Kleinschreibung wird bei Tagnamen nicht berücksichtigt. Wenn Sie zum Beispiel <code>tags= {"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" }</code> verwenden, wird <code>Tag_Name1</code> als Duplikat ignoriert. Sie können „event_type“ und „timestamp“ nicht als Tagnamen verwenden. Alle Duplikate innerhalb derselben Deklaration werden ignoriert. Tags können das APP-NAME-Feld überschreiben, wenn das Ziel ein Syslog-Server ist. Beispiel: <code>tags={"appname":"VROPS"}</code> .
exclude_fields	(Optional) Ein Parameter zum Ausschließen einzelner Felder aus der Erfassung. Sie können mehrere Werte als eine durch Semikolons getrennte Liste eingeben. Beispiel: <code>exclude_fields=hostname; filepath</code>

```
[filelog|section_name]
directory=path_to_log_directory
include=glob_pattern
```

- 3 Speichern und schließen Sie die Datei `liagent.ini`.

Beispiel: Konfigurationen

```
[filelog|messages]
directory=/var/log
include=messages;messages.?
```

```
[filelog|syslog]
directory=/var/log
include=syslog;syslog.?
```

```
[filelog|Apache]
directory=/var/log/apache2
include=*
```

Deinstallieren des Log Insight Linux Agent-RPM-Pakets

Das Log Insight Linux Agent-RPM-Paket kann deinstalliert werden.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich beim Linux-Computer an, auf dem Sie den Log Insight Linux Agent installiert haben, öffnen Sie eine Terminalkonsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass der VMware Log Insight Linux Agent installiert ist und ausgeführt wird.

Vorgehensweise

- ◆ Führen Sie den folgenden Befehl aus, wobei Sie `VERSION` und `BUILD_NUMBER` durch die Versions- und Buildnummer des installierten Agent ersetzen.

```
rpm -e VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER
```

Das Deinstallationsprogramm hält den VMware Log Insight Linux Agent-Daemon an und entfernt alle zugehörigen Dateien mit Ausnahme der eigenen Protokolle.

Deinstallieren des Log Insight Linux Agent-DEB-Pakets

Sie können das Log Insight Linux Agent-DEB-Paket deinstallieren.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich bei dem Linux-Computer an, auf dem Sie Log Insight Linux Agent installiert haben. Öffnen Sie eine Terminalkonsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass VMware Log Insight Linux Agent installiert ist und ausgeführt wird.

Vorgehensweise

- ◆ Führen Sie den folgenden Befehl aus:

```
dpkg -P vmware-log-insight-agent
```

Das Deinstallationsprogramm stoppt den VMware Log Insight Linux Agent-Daemon und entfernt all seine Dateien, mit Ausnahme seiner eigenen Protokolle, vom System.

Deinstallieren des Log Insight Linux Agent-BIN-Pakets

Das Log Insight Linux Agent-BIN-Paket kann deinstalliert werden.

Voraussetzungen

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich auf dem Linux-Computer an, auf dem Sie den Log Insight Linux Agent installiert haben, öffnen Sie eine Terminalkonsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass der VMware vRealize Log Insight Linux Agent installiert ist und ausgeführt wird.

Vorgehensweise

- 1 Halten Sie den Log Insight Linux Agent-Daemon an, indem Sie den folgenden Befehl ausführen.
`sudo service liagentd stop` oder `sudo /sbin/service liagentd stop` für ältere Distributionen.
- 2 Manuelles Entfernen der Dateien des Log Insight Linux Agent
 - `/usr/lib/loginsight-agent`: Verzeichnis für Binär- und Lizenzdateien des Daemon
 - `/var/lib/loginsight-agent`: Verzeichnis für Konfigurationsdateien und Datenbankspeicher
 - `/var/log/loginsight-agent`: Protokollverzeichnis des Log Insight Linux Agent
 - `/var/run/liagent.pid`: PID-Datei des Log Insight Linux Agent. Sollte sie nicht automatisch gelöscht werden, entfernen Sie sie manuell.
 - `/etc/init.d/liagentd`: Skriptlet-Verzeichnis des Log Insight Linux Agent-Daemon

Erstellen eines Support-Pakets für den Log Insight Linux Agent

Falls der Log Insight Linux Agent aufgrund eines Problems nicht wie erwartet funktioniert, können Sie eine Kopie der Protokoll- und Konfigurationsdateien an die VMware Support-Dienste senden.

Vorgehensweise

- 1 Melden Sie sich auf dem Zielcomputer an, auf dem der Log Insight Linux Agent installiert wurde.
- 2 Führen Sie den folgenden Befehl aus.

```
/usr/lib/loginsight-agent/bin/loginsight-agent-support
```

Das Paket wird erstellt und als ZIP-Datei im aktuellen Verzeichnis gespeichert.

Weiter

Leiten Sie das Support-Paket wie verlangt an die VMware Support-Dienste weiter.

Fehlerbehebung in den Log Insight Agents

Informationen zur Behebung bekannter Fehler können Ihnen bei der Diagnose und Behebung von Problemen bei der Bedienung von Log Insight Agents helfen.

Festlegen der Protokolldateiebene in den Log Insight Agents

Sie können die Konfigurationsdatei des Log Insight Agent bearbeiten, um die Protokollierungsebene zu ändern.

Voraussetzungen

Für den Log Insight Linux Agent:

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich beim Linux-Computer an, auf dem Sie den Log Insight Linux Agent installiert haben, öffnen Sie eine Konsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass der Log Insight Linux Agent von VMware vRealize installiert ist und ausgeführt wird.

Für den Log Insight Windows Agent:

- Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zu dem Ordner mit der Datei `liagent.ini`.

Betriebssystem	Pfad
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 Öffnen Sie die Datei `liagent.ini` in einem beliebigen Texteditor.
- 3 Ändern Sie die Debug-Protokollierungsebene im Abschnitt `[logging]` der Datei `liagent.ini`.

HINWEIS Je höher die Debug-Ebene, desto größer sind die Auswirkungen auf den Log Insight Agent. Der empfohlene Standardwert lautet 0. Debug-Ebene 1 bietet weitere Informationen und wird zur Behebung der meisten Fehler empfohlen. Debug-Ebene 2 bietet detaillierte Informationen. Verwenden Sie die Ebenen 1 und 2 nur, wenn Sie vom VMware-Support dazu aufgefordert werden.

```
[logging]
; The level of debug messages to enable: 0..2
debug_level=1
```

- 4 Speichern und schließen Sie die Datei `liagent.ini`.

Die Debug-Protokollierungsebene wurde geändert.

Keine Anzeige von Log Insight Agents auf der Benutzeroberfläche für Administratoren

Auf der Seite „Agents“ der Benutzeroberfläche für Administratoren werden keine Log Insight Agents-Instanzen angezeigt.

Problem

Nach der Installation des Log Insight Agents werden die Log Insight Agents auf der Seite „Agents“ der Benutzeroberfläche für Administratoren nicht angezeigt.

Ursache

Die gängigsten Ursachen sind Netzwerkverbindungsprobleme oder die nicht ordnungsgemäße Konfiguration des Log Insight Agents in der Datei `liagent.ini`.

Lösung

- Vergewissern Sie sich, dass das Windows- oder Linux-System, auf dem die Log Insight Agents installiert sind, mit dem Log Insight-Server verbunden ist.
- Überprüfen Sie, ob der Log Insight Agents das cfapi-Protokoll verwendet.
Bei Verwendung des Syslog-Protokolls wird Log Insight Windows Agents nicht auf der Benutzeroberfläche angezeigt.
- Zeigen Sie die Inhalte der Log Insight Agents-Protokolldateien an, die sich in den folgenden Verzeichnissen befinden.
 - Windows - %ProgramData%\VMware\Log Insight Agent\log
 - Linux - /var/log/loginsight-agent/
 Suchen Sie nach Protokollmeldungen, die die Ausdrücke `Config transport error: Couldn't resolve host name` und `Resolver failed. No such host is known` enthalten.
- Vergewissern Sie sich, dass die Datei `liagent.ini` die richtige Konfiguration für den Log Insight-Zielserver enthält. Siehe [„Festlegen des Log Insight-Zielservers“](#), auf Seite 33 und [„Festlegen des Log Insight-Zielservers“](#), auf Seite 49.

Log Insight Agents senden keine Ereignisse

Eine falsche Konfiguration kann den Log Insight Agents am Weiterleiten von Ereignissen an den Log Insight-Server hindern.

Problem

Die Log Insight Agents-Instanzen werden auf der Seite **Verwaltung > Agent** angezeigt, auf der Seite „Interaktive Analyse“ werden hinsichtlich der Log Insight Agents-Hostnamen jedoch keine Ereignisse angezeigt.

Ursache

Eine falsche Konfiguration kann die Log Insight Agents am Weiterleiten von Ereignissen an den Log Insight-Server hindern.

Lösung

- Versuchen Sie für den Log Insight Windows Agent Folgendes:
 - Rufen Sie die Inhalte der Log Insight Windows Agent-Protokolldateien unter %ProgramData%\VMware\Log Insight Agent\log auf. Suchen Sie nach Protokollmeldungen in Bezug auf die Kanalkonfiguration, welche die Ausdrücke Hat den Kanal CHANNEL_NAME abonniert enthalten. Die Standard-Kanalnamen sind Application, System und Security.
 - Wenn ein Kanal nicht korrekt konfiguriert ist, sehen Sie Protokollmeldungen wie diese: Abonnieren der Ereignisse des Kanals CHANNEL_NAME nicht möglich. Fehlercode: 15007. Der angegebene Kanal wurde nicht gefunden. Überprüfen Sie die Kanalkonfiguration. Möglicherweise sehen Sie eine andere Fehlercodenummer als 15007.
 - Wenn ein Flatfile-Erfassungskanal nicht korrekt konfiguriert ist, sehen Sie möglicherweise Meldungen wie Für den Kanal 'CHANNEL_NAME' wurden ungültige Einstellungen erhalten. Der Kanal 'CHANNEL_NAME' bleibt inaktiv, bis er ordnungsgemäß konfiguriert ist
- Versuchen Sie für Log Insight Windows Agent und Log Insight Linux Agent Folgendes:
 - ◆ Wenn kein Flatfile-Erfassungskanal konfiguriert ist, sehen Sie möglicherweise Meldungen wie Bereich 'filelog' wurde in der Konfiguration nicht gefunden. Der Flat-Dateiprotokoll-Collector bleibt inaktiv, bis er ordnungsgemäß konfiguriert wurde

Der Inhalt der Log Insight Agents-Protokolldateien befindet sich in den folgenden Verzeichnissen.

 - Windows – %ProgramData%\VMware\Log Insight Agent\log
 - Linux – /var/log/loginsight-agent/

Weiter

Weitere Informationen zur Log Insight Agents-Konfiguration finden Sie unter „[Konfigurieren des Log Insight Windows Agent nach der Installation](#)“, auf Seite 31 und unter „[Konfigurieren des Log Insight Linux Agent](#)“, auf Seite 49.

Hinzufügen einer Ausnahmeregel für den Ausgang für den Log Insight Windows Agent

Definieren Sie eine Ausnahme für die Aufhebung der Blockierung des Log Insight Windows Agent in der Windows-Firewall.

Dieses Verfahren gilt für Windows Server 2008 R2 und höher und für Windows 7 und höher.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Administratorkonto oder ein Konto mit Administratorberechtigungen verfügen.

Vorgehensweise

- 1 Wählen Sie **Start > Ausführen** aus.
- 2 Geben Sie `wf.msc` ein und klicken Sie auf **OK**.
- 3 Klicken Sie mit der rechten Maustaste im linken Fensterbereich auf **Ausgehende Regeln** und klicken Sie im linken Fensterbereich auf **Neue Regel**.

- 4 Wählen Sie **Benutzerdefiniert** aus und folgen Sie dem Assistenten, um die folgenden Optionen festzulegen.

Option	Beschreibung
Programm	liwinsvc.exe
Dienst	LogInsightAgentService
Protokolle und Ports	TCP 9000 für CFAPI und 514 für Syslog

- 5 Wählen Sie auf der Seite „Angaben der Profile, für die diese Regel angewendet wird“ den gewünschten Netzwerktyp aus.

- Domäne
- Öffentlich
- Privat

HINWEIS Sie können alle Netzwerktypen auswählen, um sicherzustellen, dass die Ausnahmeregel unabhängig vom Netzwerktyp aktiv ist.

Weiter

Navigieren Sie zum Log Insight Windows Agent-Protokollverzeichnis %ProgramData%\VMware\Log Insight Agent\log und öffnen Sie die aktuelle Protokolldatei. Wenn aktuelle Ereignisse die Meldungen Config transport error: Couldn't resolve host name und Resolver failed. No such host is known enthalten, starten Sie den Log Insight Windows Agent-Dienst und den Windows-Computer neu.

HINWEIS Es kann bis zu 5 Minuten dauern, bis der Log Insight Windows Agent-Dienst erneut eine Verbindung zum Server herstellt.

Zulassen von ausgehenden Verbindungen vom Log Insight Windows Agent in einer Windows-Firewall

Konfigurieren Sie die Einstellungen der Windows-Firewall, um ausgehende Verbindungen des Log Insight Windows Agent zum Log Insight-Server zuzulassen.

Nach der Installation des Log Insight Windows Agent-Diensts schränkt die Windows-Domäne oder die lokale Firewall die Verbindung zum Log Insight-Zielservers möglicherweise ein.

Dieses Verfahren gilt für Windows Server 2008 R2 und höher und für Windows 7 und höher.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Administratorkonto oder ein Konto mit Administratorberechtigungen verfügen.

Vorgehensweise

- 1 Wählen Sie **Start > Ausführen** aus.
- 2 Geben Sie `wf.msc` ein und klicken Sie auf **OK**.
- 3 Klicken Sie im Fensterbereich „Aktionen“ auf **Eigenschaften**.
- 4 Wählen Sie auf der Registerkarte **Domänenprofil** die Option **Zulassen (Standard)** aus dem Dropdown-Menü **Ausgehende Verbindungen** aus.

Wenn der Computer nicht mit einer Domäne verbunden ist, können Sie je nach Netzwerktyp, mit dem der Computer verbunden ist, die Option **Privates Profil** oder **Öffentliches Profil** auswählen.

- 5 Klicken Sie auf **OK**.

Weiter

Definieren Sie eine Ausnahmeregel für die Aufhebung der Blockierung für den Log Insight Windows Agent in der Windows-Firewall. Weitere Informationen hierzu finden Sie unter [„Hinzufügen einer Ausnahmeregel für den Ausgang für den Log Insight Windows Agent“](#), auf Seite 56.

Die Massenbereitstellung des Log Insight Windows Agent ist nicht erfolgreich

Die Massenbereitstellung des Log Insight Windows Agent ist auf Zielcomputern nicht erfolgreich.

Problem

Nach der Durchführung einer Massenbereitstellung auf Windows-Domänencomputern unter Verwendung von Gruppenrichtlinienobjekten schlägt die Installation von Log Insight Windows Agent als lokaler Dienst fehl.

Ursache

Gruppenrichtlinieneinstellungen verhindern die ordnungsgemäße Installation des Log Insight Windows Agent.

Lösung

- 1 Bearbeiten Sie die Einstellungen für das Gruppenrichtlinienobjekt und stellen Sie den Log Insight Windows Agent erneut bereit.
 - a Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, klicken Sie auf **Bearbeiten** und navigieren Sie zu **Computerkonfiguration > Richtlinien > Administrative Vorlagen > System > Anmeldung**.
 - b Aktivieren Sie die Richtlinie **Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten**.
 - c Navigieren Sie zu **Computerkonfiguration > Richtlinien > Administrative Vorlagen > System > Gruppenrichtlinie**.
 - d Aktivieren Sie die **Wartezeit für Richtlinienverarbeitung beim Systemstart** und legen Sie die **Wartezeit (in Sekunden)** auf 120 fest.
- 2 Führen Sie den Befehl `gpupdate /force /boot` auf den Zielcomputern aus.

Die Installation des RPM-Paket-Updates ist fehlgeschlagen

Versuche zur Installation des RPM-Paketupdates über die Linux-GUI schlagen fehl.

Problem

Die Installation bzw. das Update des Log Insight Linux Agent RPM-Pakets schlägt fehl, wenn der Vorgang in den Linux-Distributionen RHEL und SUSE über die GUI ausgeführt wird. Möglicherweise wird folgende Fehlermeldung angezeigt:

```
PK_TMP_DIR[dir:///var/tmp/TmpDir.MtqOPs] Repository ist bereits vorhanden.
```

Ursache

Es kann sein, dass der Cache und die Repository-Liste nach der Installation verschiedener Anwendungen nicht mehr leer sind.

Lösung

- 1 Melden Sie sich auf dem Linux-System an, auf dem das Log Insight Linux Agent-RPM installiert ist, und öffnen Sie eine Systemkonsole.

- 2 Führen Sie den folgenden Befehl als **Root**-Benutzer aus:

```
sudo zypper rr 2
sudo zypper rr 1
sudo zypper clean -a
sudo zypper ref
```

- 3 Doppelklicken Sie auf das Log Insight Linux Agent-RPM-Paket, um das Update zu installieren.

Log Insight Agents lehnen selbstsigniertes Zertifikat ab

Die Log Insight Agents lehnen ein selbstsigniertes Zertifikat ab.

Problem

Die Log Insight Agents lehnen ein selbstsigniertes Zertifikat ab und können keine Verbindung mit dem Server herstellen.

HINWEIS Bei Verbindungsproblemen mit dem Agent können Sie in den detaillierten Protokollen nachsehen, indem Sie die Debug-Stufe für den Log Insight Agent auf 1 ändern. Weitere Informationen hierzu finden Sie unter „[Festlegen der Protokolldateiebene in den Log Insight Agents](#)“, auf Seite 54.

Ursache

Die Meldungen im Log Insight-Agentprotokoll wurden aus bestimmten Gründen in das Protokoll eingetragen.

Meldung	Ursache
Selbstsigniertes Zertifikat wird abgelehnt. Der öffentliche Schlüssel stimmt nicht mit dem Schlüssel des vorher gespeicherten Zertifikats überein.	Dies kann vorkommen, wenn das Log Insight-Serverzertifikat ersetzt wird.
Selbstsigniertes Zertifikat wird abgelehnt. Es ist bereits ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle vorhanden.	Im Agent ist bereits ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle gespeichert.

Lösung

- ◆ Überprüfen Sie, ob es sich bei Ihrem Zielhostnamen um eine vertrauenswürdige Log Insight-Instanz handelt, und löschen Sie das frühere Zertifikat anschließend manuell aus dem Verzeichnis cert des Log Insight-Agent.
 - Log Insight Windows Agent: Navigieren Sie zu C:\ProgramData\VMware\Log Insight Agent\cert.
 - Log Insight Linux Agent: Navigieren Sie zu /var/lib/loginsight-agent/cert.

HINWEIS Auf einigen Plattformen können die Pfade der Verzeichnisse mit den vertrauenswürdigen Zertifikaten anders ausfallen. In den Log Insight Agents kann der Pfad zu den vertrauenswürdigen Zertifikaten über den Konfigurationsparameter `ssl_ca_path=<fullpath>` festgelegt werden. Ersetzen Sie <fullpath> durch den Pfad zur Paketdatei der vertrauenswürdigen Stammzertifikate. Weitere Informationen hierzu finden Sie unter „[Konfigurieren der Log Insight Agents-SSL-Parameter](#)“, auf Seite 93.

Der Log Insight -Server weist die Verbindung für nicht verschlüsselten Datenverkehr ab

Der Log Insight-Server weist die Verbindung mit dem Log Insight Agents ab, wenn Sie versuchen, nicht verschlüsselte Daten zu senden.

Problem

Wenn Sie versuchen, cfapi zum Senden von nicht verschlüsseltem Datenverkehr zu verwenden, weist der Log Insight-Server Ihre Verbindung ab. Die folgende Fehlermeldung wird im Protokoll des Log Insight-Agents vermerkt.

403 Verboten.

Ursache

Log Insight ist so konfiguriert, dass nur SSL-Verbindungen angenommen werden, aber die Log Insight Agents sind für die Verwendung einer Nicht-SSL-Verbindung konfiguriert.

Lösung

Sie können den Log Insight-Server so konfigurieren, dass Nicht-SSL-Verbindungen angenommen werden, oder Sie können den Log Insight Agents so konfigurieren, dass Daten über die SSL cfapi-Protokollverbindung gesendet werden.

Vorgehensweise

- 1 Konfigurieren Sie den Log Insight-Server so, dass Nicht-SSL-Verbindungen akzeptiert werden.
 - a Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
 - b Klicken Sie unter „Konfiguration“ auf **SSL**.
 - c Deaktivieren Sie unter „API Server SSL“ das Kontrollkästchen **SSL-Verbindung erforderlich**.
 - d Klicken Sie auf **Speichern**.
- 2 Konfigurieren Sie den Log Insight Agents so, dass Daten über die SSL Cfapi-Protokollverbindung gesendet werden.
 - a Navigieren Sie zu dem Ordner mit der Datei liagent.ini.

Betriebssystem	Pfad
Linux	/var/lib/loginsight-agent/
Windows	%ProgramData%\VMware\Log Insight Agent

- b Öffnen Sie die Datei liagent.ini in einem beliebigen Texteditor.
- c Ändern Sie den Schlüssel ssl im [Server]-Bereich der Datei liagent.ini in „Ja“ und das Protokoll in cfapi.


```
proto=cfapi
ssl=yes
```
- d Speichern und schließen Sie die Datei liagent.ini.

Clusterumgebung mit externem Lastenausgleichsmodul funktioniert nicht

Die Clusterumgebung mit einem externen Lastenausgleichsmodul, das mit Log Insight vor Version 2.5 Beta konfiguriert worden ist, funktioniert nach dem Upgrade nicht mehr.

Problem

Nach dem Upgrade auf Log Insight Agents 2.5 Beta funktioniert die Clusterumgebung mit externem Lastenausgleichsmodul nicht mehr.

Ursache

Der Log Insight Agents aus Log Insight 2.5 Beta und höher verwendet Standardeinstellungen zur Verbindung über SSL auf Port 9543. In den früheren Versionen des Log Insight Agents war die Verbindung nicht verschlüsselt.

Lösung

Sie können den Log Insight Agents für eine nicht verschlüsselte Verbindung oder das externe Lastenausgleichsmodul für SSL-Verbindungen konfigurieren.

Vorgehensweise

- 1 Konfigurieren Sie den Log Insight Agents so, dass er eine nicht verschlüsselte Verbindung verwendet.
 - a Navigieren Sie zum Ordner mit der Datei `liagent.ini`.

Betriebssystem	Pfad
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- b Öffnen Sie die Datei `liagent.ini` in einem beliebigen Texteditor.
 - c Ändern Sie im Abschnitt „`[server]`“ der Datei `liagent.ini` den SSL-Schlüssel zu 0 und den Port zu 9000.


```
port=9000
ssl=0
```
 - d Speichern und schließen Sie die Datei `liagent.ini`.
- 2 Konfigurieren Sie das externe Lastenausgleichsmodul so, dass es SSL-Verbindungen über Port 9543 übernimmt.

HINWEIS Wenn Sie mit einem Cluster arbeiten, in dem ein externes Lastenausgleichsmodul eine SSL-Verbindung abgibt, um nicht verschlüsselten Datenverkehr an Master-Knoten zu senden, stellen Sie sicher, dass das Kontrollkästchen **SSL-Verbindung erforderlich** nicht aktiviert oder der `[server]`-Konfigurationsschlüssel „`ssl`“ auf „0“ gesetzt ist. Andernfalls lehnt der Log Insight-Server die Verbindung mit den Agents ab.

Konfigurieren von Log Insight -Systemwarnungen

Administratoren können Log Insight so konfigurieren, dass Benachrichtigungen zum eigenen Systemzustand versendet werden.

Log Insight erstellt diese Benachrichtigungen, wenn ein wichtiges Systemereignis auftritt, zum Beispiel wenn der Speicherplatz fast erschöpft ist und Log Insight alte Protokolldateien löschen oder archivieren muss.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.
- 3 Stellen Sie unter dem Warnungs-Header die Systembenachrichtigungen ein.
 - a Geben Sie im Textfeld **E-Mail-Versand von Systembenachrichtigungen an** die E-Mail-Adressen ein, an die eine Benachrichtigung gesendet werden soll.
Trennen Sie mehrere E-Mail-Adressen durch Kommata.
 - b Aktivieren Sie das Kontrollkästchen **Senden einer Benachrichtigung beim Absinken der Kapazität unter** und stellen Sie den Schwellenwert ein, der den Versand der Benachrichtigungen auslöst.
 - c (Optional) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerwarnungen anhalten** nicht aktiviert ist.
Sie können dieses Kontrollkästchen aktivieren, um alle benutzerdefinierten E-Mail-Warnungen zu stoppen.

HINWEIS Systembenachrichtigungen können durch Entfernen der im Textfeld **E-Mail-Versand von Systembenachrichtigungen an** angegebenen E-Mail-Adressen deaktiviert werden (nicht empfohlen).

- 4 Klicken Sie auf **Speichern**.
- 5 Klicken Sie auf **Log Insight neu starten**, um Ihre Änderungen anzuwenden.

Von Log Insight versendete E-Mail-Benachrichtigungen

Log Insight sendet zwei Arten von E-Mail-Benachrichtigungen: Systembenachrichtigungen und benutzerdefinierte Benachrichtigungen.

Administratoren können Log Insight so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, wenn bestimmte Systemereignisse auftreten. Die Absenderadresse von Systembenachrichtigungs-E-Mails wird durch den Administratorbenutzer auf der SMTP-Konfigurationsseite der Verwaltungs-Benutzeroberfläche im Textfeld **Absender** konfiguriert. Weitere Informationen hierzu finden Sie unter [„Konfigurieren des SMTP-Servers für Log Insight“](#), auf Seite 68.

Administratorbenutzer können Log Insight auch so konfigurieren, dass Benachrichtigungs-E-Mails gesendet werden, wenn die Speicherkapazität einen festgelegten Schwellenwert unterschreitet.

Jeder Benutzer von Log Insight kann Warnungsabfragen erstellen, um E-Mail-Benachrichtigungen von Log Insight zu erhalten, wenn bestimmte Kriterien erfüllt sind.

Administratorbenutzer können alle benutzerdefinierten Benachrichtigungen deaktivieren.

Typ	Warnungsname	Beschreibung
System	Älteste Daten werden bald nicht mehr durchsuchbar sein	Diese Warnung informiert Sie, wenn in Log Insight eine Stilllegung alter Daten aus dem Speicher der virtuellen Appliance bevorsteht, und gibt die bei der aktuellen Aufnahmerate erwartete Menge durchsuchbarer Daten an. Ersetzte Daten werden archiviert, wenn Sie die Archivierung konfiguriert haben, oder andernfalls gelöscht. Die Warnung wird nach jedem Neustart des Log Insight-Diensts gesendet.
System	Repository-Aufbewahrungszeit	Diese Warnung informiert Sie über die Menge der durchsuchbaren Daten, die Log Insight bei den aktuellen Aufnahmeraten auf dem in der virtuellen Appliance verfügbaren Speicherplatz speichern kann. Admin-Benutzer können den Schwellenwert für Speicherplatzmeldungen festlegen. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Log Insight-Systemwarnungen“, auf Seite 61.
System	Verworfenne Ereignisse	Diese Warnung benachrichtigt Sie darüber, dass Log Insight nicht alle eingegangenen Protokollmeldungen aufnehmen konnte. ■ Im Falle von durch den Log Insight-Server erkannten Löschungen von TCP-Meldungen wird in beiden Fällen eine Systemwarnung in folgender Weise gesendet: ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des Log Insight-Diensts. ■ Die E-Mail enthält die Anzahl der gelöschten Meldungen seit dem Versenden der letzten Warnungs-E-Mail und die Gesamtzahl der Meldungslöschungen seit dem letzten Neustart von Log Insight. HINWEIS Die in der Zeile „Gesendet“ angegebene Uhrzeit wird durch den E-Mail-Client vorgegeben und ist die Zeit der lokalen Zeitzone, während im E-Mail-Text die UTC-Zeit angegeben wird.

Typ	Warnungsname	Beschreibung
System	Beschädigter Index-Bucket	Diese Warnung benachrichtigt Sie darüber, dass ein Teil des Festplattenindexes beschädigt ist. Ein korrupter Index weist üblicherweise auf ernsthafte Probleme im zugrunde liegenden Speichersystem hin. Der beschädigte Teil des Indexes wird von der Bedienung von Abfragen ausgeschlossen. Ein korrupter Index hat Auswirkungen auf die Aufnahme neuer Daten. Log Insight überprüft die Integrität des Indexes beim Start des Diensts. Wenn eine Beschädigung festgestellt wird, sendet Log Insight eine Systemwarnung in folgender Weise: ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des Log Insight-Diensts.
System	Zu wenig Speicherplatz	Diese Warnung benachrichtigt Sie darüber, dass Log Insight zu wenig zugewiesenen Speicherplatz hat. Diese Warnung deutet darauf hin, dass bei Log Insight wahrscheinlich ein mit dem Speicher in Verbindung stehendes Problem vorliegt.
System	Archivplatz bald voll	Diese Warnung benachrichtigt Sie darüber, dass der für die Archivierung von Log Insight-Daten verwendete Speicherplatz auf dem NFS-Server bald erschöpft ist.
System	Archivfehler	Diese Warnung benachrichtigt Sie darüber, dass ein Vorgang zur Archivierung von Log Insight-Daten auf dem NFS-Server fehlgeschlagen ist. Das bedeutet in der Regel, dass Log Insight sich nicht korrekt mit dem NFS-Server verbinden oder auf diesen schreiben kann.
System	Änderung des insgesamt bereitgestellten Festplattenspeichers	Diese Warnung benachrichtigt Sie darüber, dass sich die Gesamtgröße der Partition für die Speicherung von Log Insight-Daten verringert hat. Dies deutet in der Regel auf ein ernstes Problem im zugrunde liegenden Speichersystem hin. Wenn Log Insight diesen Umstand erkennt, wird diese Warnung in folgender Weise gesendet: ■ Sofort ■ Einmal pro Tag
System	Ausstehende Archivierungen	Diese Warnung benachrichtigt Sie darüber, dass Log Insight Daten nicht erwartungsgemäß archivieren kann. Die Warnung weist in der Regel auf Probleme mit dem von Ihnen für die Datenarchivierung konfigurierten NFS-Speicher hin.

Typ	Warnungsname	Beschreibung
System	Lizenz bald abgelaufen	Diese Warnung benachrichtigt Sie darüber, dass die Log Insight-Lizenz bald abläuft.
System	Lizenz ist abgelaufen	Diese Warnung benachrichtigt Sie darüber, dass die Log Insight-Lizenz abgelaufen ist.
System	Keine Verbindung mit dem AD-Server möglich	Mit dieser Warnmeldung werden Sie darüber in Kenntnis gesetzt, dass Log Insight keine Verbindung zum konfigurierten Active Directory-Server herstellen kann.
Benutzerdefiniert	Warnungsabfragen	Diese Warnung benachrichtigt Sie darüber, dass die Ergebnisse einer Abfrage den Kriterien entsprechen, die Sie für die Warnung festgelegt haben. Jeder Benutzer kann Warnungsabfragen festlegen, die E-Mail-Benachrichtigungen senden, wenn bestimmte Kriterien erfüllt werden. Weitere Informationen finden Sie im <i>Log Insight-Benutzerhandbuch</i> unter „Hinzufügen einer Warnungsabfrage in Log Insight, um E-Mail-Benachrichtigungen zu senden“.

Horizontalskalierungs-Systemwarnungen

Log Insight sendet spezifische Systemwarnungen, um Sie über Scale-Out-Ereignisse wie Knotenbeitritt und Mitgliedsstatusänderungen zu informieren.

Gesendet von	Warnungsname	Beschreibung
Master-Knoten	Genehmigung für neuen Worker-Knoten erforderlich	Diese Warnung benachrichtigt Sie über eine Mitgliedschaftsanforderung von einem Worker-Knoten. Die Anforderung muss von einem Admin-Benutzer genehmigt oder abgelehnt werden.
Master-Knoten	Neuer Worker-Knoten genehmigt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem Log Insight-Cluster genehmigt hat.
Master-Knoten	Neuer Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem Log Insight-Cluster abgelehnt hat. Sollte die Anforderung versehentlich abgelehnt worden sein, kann ein Admin-Benutzer diese über den Worker erneut ausgeben und sie anschließend im Master-Knoten genehmigen.
Master-Knoten	Maximale Anzahl unterstützter Knoten durch Worker-Knoten überschritten	Diese Warnung benachrichtigt Sie darüber, dass die maximal unterstützte Anzahl an Worker-Knoten im Log Insight-Cluster aufgrund eines neuen Worker-Knotens überschritten wurde.

Gesendet von	Warnungsname	Beschreibung
Master-Knoten	Zulässige Höchstzahl an Knoten überschritten, neuer Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer versucht hat, dem Cluster mehr Knoten hinzuzufügen als maximal zulässig und dass der Knoten abgelehnt wurde.
Master-Knoten	Worker-Knoten getrennt	Diese Warnung benachrichtigt Sie darüber, dass ein zuvor verbundener Worker-Knoten vom Log Insight-Cluster getrennt wurde.
Master-Knoten	Worker-Knoten erneut verbunden	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten wieder mit dem Log Insight-Cluster verbunden wurde.
Master-Knoten	Worker-Knoten von Admin widerrufen	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer die Mitgliedschaft eines Worker-Knotens widerrufen hat und der Knoten nicht mehr Teil des Log Insight-Clusters ist.
Master-Knoten	Unbekannter Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass der Log Insight-Master-Knoten die Anforderung eines Worker-Knotens abgelehnt hat, weil der Worker-Knoten dem Master-Knoten nicht bekannt war. Handelt es sich bei dem Worker-Knoten um einen gültigen Knoten, der dem Cluster hinzugefügt werden soll, melden Sie sich beim Worker-Knoten an, entfernen Sie dessen Token-Datei und Benutzerkonfiguration unter <code>/storage/core/loginsight/config/</code> und führen Sie im Worker-Knoten <code>restart loginsight service</code> aus.
Master-Knoten	Worker-Knoten ist in den Wartungsmodus übergegangen	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten in den Wartungsmodus übergegangen ist und ein Admin-Benutzer den Wartungsmodus für den Worker-Knoten deaktivieren muss, bevor Änderungen an der Konfiguration des Worker-Knotens vorgenommen werden können und dieser Abfragen verarbeiten kann.
Master-Knoten	Worker-Knoten wieder betriebsbereit	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten den Wartungsmodus verlassen hat und wieder betriebsbereit ist.

Gesendet von	Warnungsname	Beschreibung
Worker-Knoten	Master ausgefallen oder vom Worker-Knoten getrennt	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten, der die Warnung sendet, keinen Kontakt zum Log Insight-Master-Knoten herstellen kann. Dies könnte möglicherweise bedeuten, dass der Master-Knoten ausgefallen ist und gegebenenfalls neu gestartet werden muss. Bei einem Ausfall des Master-Knotens kann der Cluster nicht konfiguriert werden und es können keine Abfragen übermittelt werden, bis dieser wieder online ist. Worker-Knoten nehmen weiterhin Nachrichten auf. HINWEIS Sie könnten möglicherweise viele solcher Warnungen erhalten, weil mehrere Worker-Knoten den Ausfall des Master-Knotens unabhängig voneinander registrieren und entsprechende Benachrichtigungen ausgeben könnten.
Worker-Knoten	Master-Knoten mit Worker-Knoten verbunden	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten, der die Warnung sendet, wieder mit dem Log Insight-Master-Knoten verbunden ist.

Synchronisieren der Uhrzeit der virtuellen Log Insight -Appliance

Die Uhrzeit der virtuellen Log Insight-Appliance muss mit einem NTP-Server oder dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben, synchronisiert werden.

Die Uhrzeit ist für die Kernfunktionalität von Log Insight von entscheidender Bedeutung.

Log Insight synchronisiert standardmäßig die Uhrzeit mit einer vordefinierten Liste öffentlicher NTP-Server. Sollten öffentliche NTP-Server aufgrund einer Firewall nicht zugänglich sein, können Sie den internen NTP-Server Ihres Unternehmens nutzen. Wenn keine NTP-Server verfügbar sind, können Sie die Uhrzeit mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle Log Insight-Appliance bereitgestellt haben, synchronisieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **Uhrzeit**.
- 3 Wählen Sie im Dropdown-Menü **Uhrzeit synchronisieren mit** die Zeitquelle aus.

Option	Beschreibung
NTP-Server	Synchronisiert die Uhrzeit der virtuellen Log Insight-Appliance mit der Uhrzeit eines der aufgeführten NTP-Server.
ESX/ESXi-Host	Synchronisiert die Uhrzeit der virtuellen Log Insight-Appliance mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben.

- 4 (Optional) Wenn Sie NTP-Server-Synchronisation ausgewählt haben, listen Sie die NTP-Server-Adressen auf und klicken Sie auf **Testen**.

HINWEIS Das Testen der Verbindung zu NTP-Servern kann bis zu 20 Sekunden pro Server in Anspruch nehmen.

- 5 Klicken Sie auf **Speichern**.

Konfigurieren des SMTP-Servers für Log Insight

Sie können einen SMTP so konfigurieren, dass das Versenden von E-Mail-Warnungen durch Log Insight zugelassen wird.

Systemwarnungen werden erzeugt, wenn Log Insight ein wichtiges Systemereignis erkennt, zum Beispiel wenn die Speicherkapazität der virtuellen Appliance die von Ihnen festgelegten Schwellenwerte erreicht hat. Weitere Informationen hierzu finden Sie unter „[Von Log Insight versendete E-Mail-Benachrichtigungen](#)“, auf Seite 62.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter "Konfiguration" auf **SMTP**.
- 3 Geben Sie die SMTP-Server-Adresse und die Portnummer ein.
- 4 Wenn der SMTP-Server eine verschlüsselte Verbindung verwendet, wählen Sie das Verschlüsselungsprotokoll aus.
- 5 Geben Sie im Textfeld **Absender** eine E-Mail-Adresse ein, die beim Versenden von Systemwarnungen verwendet werden soll.

Die **Absender**-Adresse erscheint als die Adresse des Absenders in den Systembenachrichtigungs-E-Mails. Sie muss keine echte Adresse sein und kann durch ihren Namen auf eine spezifische Instanz von Log Insight hinweisen. Beispiel: **loginsight@beispiel.com**.
- 6 Geben Sie einen Benutzernamen und ein Kennwort zur Authentifizierung beim SMTP-Server beim Versenden von Systemwarnungen ein.
- 7 Geben Sie eine Ziel-E-Mail-Adresse ein und klicken Sie auf **Test-E-Mail senden**, um die Verbindung zu überprüfen.
- 8 Klicken Sie auf **Speichern**.

Integration von Log Insight in andere VMware-Produkte

Log Insight kann in andere VMware-Produkte integriert werden, um Ereignisse und Protokolldaten zu verwenden und einen besseren Überblick über die in Ihrer virtuellen Umgebung auftretenden Ereignisse zu bieten.

Integration in VMware vSphere

Log Insight-Administratorbenutzer können Log Insight so einrichten, dass alle zwei Minuten eine Verbindung mit vCenter Server hergestellt wird und Ereignis-, Warnungs- und Aufgabendaten dieser vCenter Server-Systeme gesammelt werden. Außerdem kann Log Insight ESXi-Hosts über vCenter Server konfigurieren. Weitere Informationen hierzu finden Sie unter [„Verbinden von Log Insight mit einer vSphere-Umgebung“](#), auf Seite 70.

Integration in VMware vRealize Operations Manager

Sie können Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in Log Insight finden Sie in der Anleitung *Erste Schritte für Log Insight*.

Log Insight und vRealize Operations Manager lassen sich auf zwei unabhängige Weisen integrieren.

Benachrichtigungse-reignisse

Log Insight-Administratorbenutzer können Log Insight so einrichten, dass auf von Ihnen erstellten Abfragen basierende Benachrichtigungsereignisse an vRealize Operations Manager gesendet werden. Diese Benachrichtigungsereignisse sind in vRealize Operations Manager keine Warnungen und haben keinen Einfluss auf die Werte der Badges „Systemzustand“, „Risiko“ oder „Effizienz“. Weitere Informationen hierzu finden Sie unter [„Konfigurieren von Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager“](#), auf Seite 76.

Kontextbezogener Start

Kontextbezogener Start ist eine Funktion in vRealize Operations Manager, die es Ihnen ermöglicht, in einem bestimmten Kontext eine externe Anwendung per URL zu starten. Der Kontext wird durch das aktive Benutzeroberflächenelement und die Objektauswahl definiert. Über den kontextbezogenen Start kann der Log Insight-Adapter einer Reihe verschiedener Ansichten innerhalb der benutzerdefinierten Benutzeroberfläche und der vSphere-Benutzeroberfläche von vRealize Operations Manager Menüelemente hinzufügen. Weitere Informationen hierzu finden Sie unter [„Aktivieren des kontextbezogenen Starts für Log Insight in vRealize Operations Manager“](#), auf Seite 80.

HINWEIS Benachrichtigungsereignisse hängen nicht von der Konfiguration des kontextbezogenen Starts ab. Sie können Benachrichtigungsereignisse auch dann von Log Insight an vRealize Operations Manager senden, wenn Sie die Funktion Kontextbezogener Start nicht aktivieren.

Wenn sich die Umgebung verändert, können Administratorbenutzer von Log Insight vSphere-Systeme ändern, hinzufügen oder aus Log Insight entfernen, die vRealize Operations Manager-Instanz ändern oder entfernen, an die Warnungsbearbeitungen gesendet werden, und die zur Verbindung von vSphere-Systemen und vRealize Operations Manager verwendeten Kennwörter ändern.

Verbinden von Log Insight mit einer vSphere-Umgebung

Bevor Sie Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus Ihrer vSphere-Umgebung konfigurieren, müssen Sie Log Insight mit einem oder mehreren vCenter Server-Systemen verbinden.

Log Insight kann zwei Arten von Daten aus vCenter Server-Instanzen und den ESXi-Hosts, die sie verwalten, erfassen.

- Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Nach erfolgter Konfiguration ruft Log Insight Ereignisse, Aufgaben und Warnungen der registrierten vCenter Server-Instanzen ab.
- Protokolle enthalten unstrukturierte Daten, die in Log Insight analysiert werden können. ESXi-Hosts oder vCenter Server Appliance-Instanzen können ihre Protokolle über Syslog an Log Insight übermitteln.

Voraussetzungen

- Vergewissern Sie sich, dass Sie für den gewünschten Integrationsgrad über Anmeldedaten mit ausreichenden Rechten verfügen, um die erforderliche Konfiguration am vCenter Server-System und dessen ESXi-Hosts vorzunehmen.

Integrationsgrad	Erforderliche Berechtigungen
Erfassung von Ereignissen, Aufgaben und Alarmen	■ System.Anzeigen HINWEIS System.Anzeigen ist eine systemdefinierte Berechtigung. Wenn Sie eine benutzerdefinierte Rolle hinzufügen, ohne ihr Berechtigungen zuzuweisen, wird sie als schreibgeschützte Rolle mit drei systemdefinierten Berechtigungen erstellt: System.Anonym, System.Anzeigen und System.Lesen.
Syslog-Konfiguration auf ESXi-Hosts	■ Host.Konfiguration.Einstellungen ändern ■ Host.Konfiguration.Netzwerkkonfiguration

HINWEIS Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

- Sie müssen die IP-Adresse oder den Domännennamen des vCenter Server-Systems kennen.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Geben Sie die IP-Adresse und die Anmeldedaten für einen vCenter Server ein und klicken Sie auf **Verbindung testen**.

Die Verwendung von Anmeldedaten für das Dienstkonto wird empfohlen.

- 4 (Optional) Klicken Sie, um einen weiteren vCenter Server zu registrieren, auf **vCenter Server hinzufügen** und wiederholen Sie die Schritte 3 bis 5.

HINWEIS Registrieren Sie keine vCenter Server-Systeme mit doppelt vorhandenen Namen oder IP-Adressen. Log Insight prüft nicht, ob vCenter Server-Namen doppelt vorhanden sind. Sie müssen sicherstellen, dass die Liste der registrierten vCenter Server-Systeme keine doppelten Einträge enthält.

- 5 Klicken Sie auf **Speichern**.

Weiter

- Starten Sie die Erfassung von Ereignis-, Aufgaben- und Warnungsdaten aus der vCenter Server-Instanz, die Sie registriert haben. Weitere Informationen hierzu finden Sie unter „[Konfigurieren von Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server-Instanzen](#)“, auf Seite 71.
- Starten Sie die Erfassung von Syslog-Feeds von den durch vCenter Server verwalteten ESXi-Hosts. Weitere Informationen hierzu finden Sie unter „[Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an Log Insight](#)“, auf Seite 72.

Konfigurieren von Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server -Instanzen

Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Sie können Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus einem oder mehreren vCenter Server-Systemen konfigurieren.

Über die Administrations-Benutzeroberfläche können Sie Log Insight für die Verbindung mit vCenter Server-Systemen konfigurieren. Die Informationen werden von den vCenter Server-Systemen mithilfe der vSphere Web Services-API abgerufen und in der Web-Benutzeroberfläche von Log Insight als vSphere-Inhaltspaket angezeigt.

HINWEIS Log Insight kann Warnungs-, Ereignis- und Aufgabendaten nur von vCenter Server 5.1 und höher abrufen.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Anmeldedaten mit **System.View**-Berechtigungen verfügen.

HINWEIS Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Suchen Sie die vCenter Server-Instanz, aus der Sie Daten erfassen möchten, und aktivieren Sie das Kontrollkästchen **vCenter Server-Ereignisse, -Aufgaben und -Warnungen sammeln**.
- 4 Klicken Sie auf **Speichern**.

Log Insight verbindet sich alle zwei Minuten mit vCenter Server und bezieht alle neuen Informationen seit dem letzten Abruf.

Weiter

- Analysieren Sie vSphere-Ereignisse mit dem vSphere-Inhaltspaket oder mittels benutzerdefinierter Abfragen.
- Aktivieren Sie Inhaltspaketwarnungen oder benutzerdefinierte Benachrichtigungen für vSphere.

Log Insight als Syslog-Server

Log Insight umfasst einen integrierten Syslog-Server, der während der Ausführung des Log Insight-Diensts andauernd aktiv ist.

Der Syslog-Server überwacht die Ports 514/TCP, 1514/TCP und 514/UDP und kann Protokollnachrichten anderer Hosts aufnehmen. Vom Syslog-Server aufgenommene Nachrichten können in der Log Insight-Web-Benutzeroberfläche nahezu in Echtzeit durchsucht werden. Damit Log Insight die Syslog-Nachrichten akzeptieren kann, dürfen sie nicht größer als 10 KB sein.

Konfigurieren eines ESXi -Hosts für die Weiterleitung von Protokollereignissen an Log Insight

Protokolle enthalten unstrukturierte Daten, die in Log Insight analysiert werden können. ESXi-Hosts oder vCenter Server Appliance-Instanzen können ihre Protokolle über Syslog an Log Insight übermitteln.

Sie müssen die ESXi-Hosts oder vCenter Server Appliance-Instanzen so konfigurieren, dass ihre Syslog-Daten an Log Insight übermittelt werden.

Ein Log Insight-Cluster kann einen Lastausgleichsdienst verwenden, um Syslog-Feeds von ESXi und vCenter Server Appliance auf die einzelnen Knoten des Clusters zu verteilen.

Über die Verwaltungs-Benutzeroberfläche von Log Insight können Sie ESXi-Hosts auf einem registrierten vCenter Server so konfigurieren, dass sie Syslog-Feeds an Log Insight weiterleiten.



VORSICHT Das Ausführen paralleler Konfigurationsaufgaben kann möglicherweise zu fehlerhaften Syslog-Einstellungen auf dem ESXi-Zielhost führen. Stellen Sie sicher, dass kein anderer Administratorbenutzer eine Konfiguration an den ESXi-Hosts vornimmt, die Sie konfigurieren möchten.

Informationen zur Konfiguration von Syslog-Feeds über eine vCenter Server Appliance finden Sie unter [„Konfigurieren einer vCenter Server Appliance für das Weiterleiten von Protokollereignissen an Log Insight“](#), auf Seite 75.

HINWEIS Log Insight kann Syslog-Daten von ESXi-Hosts der Versionen 5.x und höher empfangen.

Voraussetzungen

- Stellen Sie sicher, dass der vCenter Server, der den ESXi-Host verwaltet, bei Ihrer Log Insight-Instanz registriert ist.
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
 - **Host.Konfiguration.Erweiterte Einstellungen**
 - **Host.Konfiguration.Sicherheitsprofil und Firewall**

HINWEIS Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Suchen Sie die vCenter Server-Instanz, die den ESXi-Host, von dem Sie Syslog-Feeds erhalten möchten, verwaltet.

- 4 Aktivieren Sie das Kontrollkästchen **ESXi-Hosts für das Versenden von Protokollen an Log Insight konfigurieren**.

Log Insight konfiguriert standardmäßig alle erreichbaren ESXi-Hosts der Versionen 5.x und höher so, dass sie ihre Protokolle über UDP senden. ESX-Hosts werden nicht unterstützt.

- 5 (Optional) Geben Sie den Hostnamen oder die IP-Adresse eines Lastausgleichsdienstes an, den Sie zum Verteilen von Syslog-Feeds verwenden möchten.
- 6 (Optional) Klicken Sie, um auszuwählen, welche ESXi-Hosts ihre Protokolle an Log Insight weiterleiten, welches Übertragungsprotokoll für die Weiterleitung von Protokollen an Log Insight verwendet wird und wie die Syslog-Konfiguration auf ESXi 5.x-Hosts erfolgen soll, auf **Erweiterte Optionen**.
- 7 Klicken Sie auf **Speichern**.

Manuelle Syslog-Konfiguration über vSphere Web Client

Sie können über vSphere Web Client Syslog auf einem ESXi-Host so konfigurieren, dass Protokollmeldungen an Log Insight weitergeleitet werden.

Um Protokollmeldungen von mehreren ESXi-Hosts auf dem vCenter Server an Log Insight weiterzuleiten, müssen Sie jeden einzelnen ESXi-Host konfigurieren.

HINWEIS Die Vorgehensweise variiert möglicherweise je nach zu konfigurierendem ESXi-Host und verwendetem vSphere Web Client .

Voraussetzungen

HINWEIS Wenn Sie einen ESXi-Host bereits zum Weiterleiten von Protokollereignissen an Log Insight anhand des Verfahrens „[Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an Log Insight](#)“, auf Seite 72 konfiguriert haben, können Sie das Verfahren zur manuellen Konfiguration ignorieren.

- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
 - **Host.Konfiguration.Erweiterte Einstellungen**
 - **Host.Konfiguration.Sicherheitsprofil und Firewall**

HINWEIS Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bezeichnungsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

- Überprüfen Sie, ob Sie bei dem vCenter Server angemeldet sind, der den ESXi-Host verwaltet, den Sie konfigurieren möchten.

Vorgehensweise

- 1 Wählen Sie im Objektnavigator den ESXi-Host, den Sie konfigurieren möchten, und klicken Sie auf die Registerkarte **Verwalten**.
- 2 Klicken Sie auf der Registerkarte **Einstellungen** auf **Erweiterte Systemeinstellungen**.
- 3 Suchen Sie die Eigenschaft Syslog.global.logHost und klicken Sie auf das Symbol **Bearbeiten** .

- 4 Ändern Sie die Eigenschaft Syslog.global.logHost so, dass sie auf die IP-Adresse oder den Hostnamen von Log Insight verweist, und klicken Sie auf **OK**.

Das URL-Format lautet `tcp|udp|ssl://log_insight-host:514|1514`, wobei *log_insight-host* die IP-Adresse bzw. der Hostname der virtuellen Log Insight-Appliance ist.

HINWEIS Verwenden Sie Port 514 für UDP- und TCP-Kommunikation und Port 1514 für das SSL-Protokoll.

- 5 Stellen Sie sicher, dass die Firewall nicht die Kommunikationsports blockiert.
 - a Klicken Sie auf der Registerkarte **Einstellungen** auf **Sicherheitsprofil** und überprüfen Sie, ob Syslog in der Liste „Ausgehende Verbindungen“ erscheint.
 - b Wenn Sie Syslog nicht in der Liste „Ausgehende Verbindungen“ sehen, klicken Sie oben rechts auf **Bearbeiten**.
 - c Scrollen Sie in der Dienste-Liste nach unten, bis Sie den Syslog-Dienst finden, und aktivieren Sie das Kontrollkästchen **Syslog**.
 - d Klicken Sie auf **OK**.

Manuelle Syslog-Konfiguration per Befehlszeile

Sie können Syslog mit dem Dienstprogramm `esxcli` zum Weiterleiten von Protokollereignissen an Log Insight konfigurieren.

Sie können den `esxcli`-Befehl in der Konsole eines ESXi-Hosts, in der vSphere-Befehlszeilenschnittstelle oder im vSphere Management Assistant ausführen.

Voraussetzungen

HINWEIS Wenn Sie einen ESXi-Host bereits zum Weiterleiten von Protokollereignissen an Log Insight anhand des Verfahrens „[Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an Log Insight](#)“, auf Seite 72 konfiguriert haben, können Sie das Verfahren zur manuellen Konfiguration ignorieren.

- Wenn Sie einen ESXi-Host der Version 5.x konfigurieren möchten, lesen und beachten Sie die Informationen im VMware-Knowledgebase-Artikel [Konfiguration von Syslog auf ESXi 5.x \(KB 2003322\)](#).
- Wenn Sie einen ESXi-Host der Version 4.x konfigurieren möchten, lesen und beachten Sie die Informationen im VMware-Knowledgebase-Artikel [Aktivieren von Syslog auf ESXi 3.5 und 4.x \(KB 1016621\)](#).
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
 - **Host.Konfiguration.Erweiterte Einstellungen**
 - **Host.Konfiguration.Sicherheitsprofil und Firewall**

HINWEIS Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

- 1 Öffnen Sie eine ESXi-Shell-Konsolensitzung, in der der Befehl `esxcli` zur Verfügung steht.
Sie können beispielsweise vMA verwenden oder die Sitzung direkt auf dem ESXi-Host öffnen.
- 2 Führen Sie den folgenden Befehl aus, um die aktuellen Konfigurationsoptionen auf dem Host anzuzeigen:
`esxcli system syslog config get`

- Um eine Host-Konfiguration zu ändern, führen Sie den folgenden Befehl zur Angabe der zu ändernden Optionen aus:

```
esxcli system syslog config set --loghost=tcp|udp|ssl://log_insight-host:514
```

HINWEIS Sie müssen `udp` oder `tcp` verwenden. Sie dürfen jedoch nicht beide verwenden.

Der folgende Befehl konfiguriert Remote-Syslog beispielsweise zur Verwendung von `udp` auf Port 514.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514
```

Um Ihren ESXi-Host für das Weiterleiten von Protokollen an mehrere Endpunkte zu konfigurieren, können Sie die Endpunkte durch Kommata getrennt im Befehl auflisten.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514,tcp://192.168.100.101:514
```

- Führen Sie, um sicherzustellen, dass die ESXi-Firewall so konfiguriert ist, dass der Syslog-Datenverkehr den Host verlassen darf, folgende Befehle aus:

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
esxcli network firewall refresh
```

- Laden Sie die neue Konfiguration, indem Sie den Befehl `esxcli system syslog reload` ausführen.

HINWEIS Wenn Sie diesen Befehl nicht ausführen, wird die Konfigurationsänderung nicht wirksam.

Konfigurieren einer vCenter Server Appliance für das Weiterleiten von Protokollereignissen an Log Insight

Sie können eine vCenter Server Appliance so konfigurieren, dass diese ihre Protokollmeldungen über Syslog an Log Insight sendet.

Informationen zur Konfiguration von ESXi-Hosts zur Weiterleitung ihrer Protokolle an Log Insight finden Sie im Abschnitt *Log Insight mit vCenter Server 5.1.x-Systemen verbinden* des Log Insight-Administratorhandbuchs.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten für die vCenter Server Appliance verfügen.
- Wenn Sie eine Verbindung zu einer virtuellen Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

- Stellen Sie eine SSH-Verbindung zum vCenter Server Appliance-Host her und melden Sie sich als Root-Benutzer an.
- Navigieren Sie zu `/etc/syslog-ng/`.
- Öffnen Sie die Datei `syslog-ng.conf` zur Bearbeitung und fügen Sie am Ende der Datei den folgenden Text hinzu:

```
source vpxd {
file("/var/log/vmware/vpx/vpxd.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vpxd-alert.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vws.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vmware-vpxd.log" follow_freq(1) flags(no-parse));
```

```
file("/var/log/vmware/vpx/inventoryservice/ds.log" follow_freq(1) flags(no-parse));
};
destination loginsight { udp("<loginsight-host>"); };
log { source(vpxd); destination(loginsight); };
```

HINWEIS Sie können tcp statt udp verwenden.

- 4 Führen Sie `service syslog restart` aus, um die neue Konfiguration zu laden.

Konfigurieren von Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager

Sie können Log Insight konfigurieren, um Warnungsbenachrichtigungen an vRealize Operations Manager zu senden.

Sie können Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in Log Insight finden Sie in der Anleitung *Erste Schritte für Log Insight*.

Bei der Integration von Log Insight-Warnungen mit vRealize Operations Manager können Sie alle Informationen über Ihre Umgebung in einer einzelnen Benutzeroberfläche anzeigen.

Sie können Benachrichtigungsereignisse von mehreren Log Insight-Instanzen aus an eine einzelne vRealize Operations Manager-Instanz senden. Sie können den kontextbezogenen Start für eine einzelne Log Insight-Instanz pro vRealize Operations Manager-Instanz aktivieren.

Voraussetzungen

- Vergewissern Sie sich, dass die Version von vRealize Operations Manager Warnungsbenachrichtigungen von Log Insight unterstützt. Weitere Informationen zu unterstützten Produktversionen finden Sie in der Anleitung *Erste Schritte für Log Insight* unter „Produktkompatibilität“.

HINWEIS Log Insight überprüft nicht die Version auf dem Ziel-vRealize Operations Manager und Sie können die Konfiguration der Benachrichtigungen fortsetzen. Die Benachrichtigungsereignisse werden jedoch möglicherweise nicht wie erwartet auf der vRealize Operations Manager-Benutzeroberfläche angezeigt.

- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

HINWEIS Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

- Sie müssen die IP-Adresse oder den Hostnamen der Ziellinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.

- 2 Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.
- 3 Geben Sie die IP-Adresse oder den Host- Namen sowie die Anmeldedaten für die virtuelle Maschine der Benutzeroberfläche der vRealize Operations Manager-Instanz ein und klicken Sie auf **Testverbindung**.

Log Insight verwendet Anmeldedaten, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden. Die Verwendung von Anmeldedaten für das Dienstkonto wird empfohlen.
- 4 Wählen Sie im Bereich „vRealize Operations Manager“ **Integration von Warnungen aktivieren** aus.
- 5 Klicken Sie auf **Speichern**.

Weiter

- Die von Log Insight gesendeten Benachrichtigungsereignisse werden auf der vSphere-Benutzeroberfläche von vRealize Operations Manager nicht standardmäßig angezeigt. Navigieren Sie zu **Planung > Ereignisse** und klicken Sie auf **Benachrichtigungsereignisse zeigen**.
- Sie können Warnungsabfragen zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager konfigurieren. Weitere Informationen finden Sie unter dem Thema „Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse zu senden“ im vRealize Operations Manager *Log Insight-Benutzerhandbuch*.

Log Insight -Benachrichtigungsereignisse in vRealize Operations Manager

Sie können Log Insight konfigurieren, damit Benachrichtigungsereignisse an vRealize Operations Manager auf Basis der von Ihnen erstellten Warnungsabfragen gesendet werden.

Wenn Sie eine Benachrichtigungswarnung in Log Insight konfigurieren, wählen Sie eine Ressource in vRealize Operations Manager aus, die den Benachrichtigungsereignissen zugeordnet ist. Weitere Informationen finden Sie unter „Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden“ im *Log Insight-Benutzerhandbuch*.

Der Speicherort der Log Insight-Benachrichtigungsereignisse hängt von der verwendeten Benutzeroberflächenversion von vRealize Operations Manager ab.

Tabelle 1-1. Bereiche der Benutzeroberfläche von vRealize Operations Manager , in denen Benachrichtigungsereignisse angezeigt werden

vRealize Operations Manager-Benutzeroberfläche	Bereiche, in denen Log Insight-Benachrichtigungsereignisse angezeigt werden
Benutzerdefinierte Benutzeroberfläche	■ Seite „Warnungen – Übersicht“. ■ Alle Dashboards, in denen das Dashboard-Widget „Warnungen“ angezeigt wird
vSphere-Benutzeroberfläche	■ Registerkarte Ereignisse unter der Registerkarte Vorgänge ■ Registerkarte Ereignisse unter der Registerkarte Planung

Der Name und die Beschreibung der Warnung, die Sie in Log Insight angegeben haben, werden in der Spalte „Warnungsinformationen“ der Warnungsliste in vRealize Operations Manager angezeigt.

In der benutzerdefinierten Benutzeroberfläche ist die Spalte „Warnungsinformationen“ standardmäßig nicht sichtbar. Sie können die Spalte „Warnungsinformationen“ aktivieren, indem Sie das Dropdown-Menü in der Tabellenkopfzeile erweitern und das Kontrollkästchen **Warnungsinformationen** aktivieren.

Hinzufügen einer Suchdomäne

Sie können eine Suchdomäne hinzufügen, um den vRealize Operations Manager-Inventarabgleich zu optimieren.

Durch das Hinzufügen einer Suchdomäne wird der Abgleich, wenn die Beschriftungs- und Suchdomäne einer virtuellen Maschine in Bezug auf die IP-Adresse des Hosts aufgelöst wird, welcher Protokollmeldungen an Log Insight sendet, verbessert. Beispiel: Wenn Sie über eine virtuelle Maschine mit der Bezeichnung linux_01 in vRealize Operations Manager verfügen und wenn der Hostname linux_01.company.com in 192.168.10.10 aufgelöst wird, kann Log Insight durch das Hinzufügen einer Suchdomäne diese Ressource erkennen und abgleichen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden. Siehe „[Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance](#)“, auf Seite 8.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur virtuellen Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
- 2 Öffnen Sie `/etc/resolv.conf`.
- 3 Geben Sie Ihre Suchdomäne ein. Beispiel: `search company.com`.
- 4 Speichern und schließen Sie die Datei.

Installieren des Log Insight -Adapters in der Standalone-Version von vRealize Operations Manager

Sie können den Log Insight-Adapter in der Standalone-Version von vRealize Operations Manager installieren, um den kontextbezogenen Start zu aktivieren.

Der Log Insight-Adapter liefert vRealize Operations Manager die notwendigen Informationen, um Log Insight zu starten. Dieser Adapter sammelt keine Daten.

Der Log Insight-Adapter wird als Teil der vRealize Operations Manager 5.7.1-vApp, nicht jedoch als Teil der Standalone-Version von vRealize Operations Manager installiert. Daher müssen Sie für die Standalone-Version den Log Insight-Adapter manuell installieren.

Der Log Insight-Adapter ist als Teil von vRealize Operations Manager 5.7.2 und 5.8 installiert.

VMware verteilt den Log Insight-Adapter als `.tgz`-Archiv, das die Installationsprogramme für Windows und Linux enthält.

Voraussetzungen

- Laden Sie die Management Pack-Installationsdatei von https://solutionexchange.vmware.com/store/category_groups/cloud-management herunter. Sie können die TGZ-Datei über die Registerkarte „Ressourcen“ der Management-Pack-Seite herunterladen.
- Notieren Sie sich die Build-Nummer im Namen TGZ-Datei. Die Build-Nummer wird nach dem Namen des Management Packs angezeigt, zum Beispiel `managementpack_name-buildnumber.tgz`.
- Stellen Sie sicher, dass Sie Zugriff auf den Server haben, auf dem vRealize Operations Managerausgeführt wird, und dass Sie über die entsprechenden Berechtigungen verfügen, um Software auf dem Server installieren.

- Vergewissern Sie sich, dass die Version von vRealize Operations Manager 5.7.1 oder höher ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

HINWEIS Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

Vorgehensweise

- 1 Öffnen Sie die TGZ-Datei und extrahieren Sie die TAR-Datei an einem temporären Speicherort auf Ihrem vRealize Operations Manager-Server.
 - 2 Öffnen Sie im temporären Ordner die TAR-Datei und extrahieren und führen Sie das Installationsprogramm für Ihre Betriebssystemplattform aus.
 - 3 Melden Sie sich bei vRealize Operations Manager als Administrator an.
 - 4 Wählen Sie **Admin > Support** aus.
 - 5 Suchen Sie auf der Registerkarte **Info** den Bereich „Adapterinformationen“ und klicken Sie auf das Symbol **Beschreiben** (📄).
- Das **Describe**-Symbol befindet sich oben rechts im Bereich „Adapterinformationen“.
- 6 Klicken Sie auf **Ja**, um den Describe-Vorgang zu starten.
 - 7 Überprüfen Sie, ob die Build-Nummer in der Spalte „Adapterversion“ für das Management Pack mit der Build-Nummer in der TGZ-Datei übereinstimmt, die Sie heruntergeladen haben.

Weiter

Aktivieren Sie nach der Installation des Adapters den kontextbezogenen Start über die Verwaltungs-Web-Benutzeroberfläche von Log Insight.

Weitere Informationen finden Sie unter *Aktivieren des kontextbezogenen Starts für Log Insight in vRealize Operations Manager* im *Log Insight-Administratorhandbuch*.

vRealize Operations Manager -Inhaltspaket für Log Insight

Das vRealize Operations Manager-Inhaltspaket für Log Insight enthält Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die zur Analyse aller von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle verwendet werden.

Das vRealize Operations Manager-Inhaltspaket bietet die Möglichkeit, alle von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle zu analysieren. Das Inhaltspaket enthält Dashboards, Abfragen und Warnungen, die dem vRealize Operations Manager-Administrator die Diagnose und Fehlerbehebung ermöglichen sollen. Die Dashboards sind zur besseren Verwaltbarkeit nach den Hauptkomponenten von vRealize Operations Manager wie Analyse, Benutzeroberfläche und Adapter gruppiert. Sie können verschiedene Alarme für das Versenden von Benachrichtigungsereignissen in vRealize Operations Manager und von E-Mails an Administratoren aktivieren.

HINWEIS Für das Inhaltspaket von vRealize Operations Manager sind Log Insight Version 1.5 und vRealize Operations Manager Version 5.8 erforderlich.

Das Inhaltspaket von vRealize Operations Manager kann über https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US heruntergeladen werden.

Siehe unter „Arbeiten mit Inhaltspaketen“ im *Log Insight-Benutzerhandbuch*.

Aktivieren des kontextbezogenen Starts für Log Insight in vRealize Operations Manager

Sie können vRealize Operations Manager so konfigurieren, dass mit Log Insight in Zusammenhang stehende Menüelemente angezeigt werden und Log Insight mit einer objektspezifischen Abfrage gestartet wird.

Sie können Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in Log Insight finden Sie in der Anleitung *Erste Schritte für Log Insight*.

WICHTIG Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von Log Insight. Da Log Insight nicht überprüft, ob bei vRealize Operations Manager bereits andere Instanzen registriert sind, könnten Sie die Einstellungen eines anderen Benutzers außer Kraft setzen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

HINWEIS Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

- Vergewissern Sie sich, dass die Version von vRealize Operations Manager 5.7.1 oder höher ist.

HINWEIS Log Insight überprüft die Zielversion von vRealize Operations Manager nicht und ermöglicht es Ihnen, fortzufahren. Jedoch ist vRealize Operations Manager 5.7.1 oder höher erforderlich, damit die Verknüpfung zurück zu Log Insight funktioniert und die Warnung geöffnet wird, die das Benachrichtigungseignis generiert hat.

Weitere Informationen zu unterstützten Produktversionen finden Sie in der Anleitung *Erste Schritte für Log Insight* unter "Produktkompatibilität".

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.

- 3 Geben Sie die IP-Adresse oder den Host- Namen sowie die Anmeldedaten für die virtuelle Maschine der Benutzeroberfläche der vRealize Operations Manager-vApp ein, und klicken Sie auf **Verbindung testen**.

HINWEIS Sie müssen die Benutzeranmeldedaten eines vRealize Operations Manager-Administrators eingeben.

- 4 Klicken Sie auf **Speichern**.

Log Insight konfiguriert die vRealize Operations Manager-Instanz. Dieser Vorgang kann einige Minuten dauern.

Es werden mit Log Insight in Zusammenhang stehende Elemente in den Menüs von vRealize Operations Manager angezeigt.

Weiter

Starten Sie eine Log Insight-Abfrage aus der vRealize Operations Manager-Instanz. Siehe „[Kontextbezogener Start von Log Insight](#)“, auf Seite 81.

Kontextbezogener Start von Log Insight

Sie können vRealize Operations Manager 5.7.1 oder höher konfigurieren, um Aktionen in Verbindung mit Log Insight auszulösen.

Wenn Sie den kontextbezogenen Start für Log Insight aktivieren, wird eine Log Insight-Ressource unter dem HTTP-Post-Adapter in vRealize Operations Manager erstellt. Der Ressourcenbezeichner enthält die IP-Adresse der Log Insight-Instanz und wird von vRealize Operations Manager zum Öffnen von Log Insight verwendet.

Kontextbezogener Start in der vSphere-Benutzeroberfläche von vRealize Operations Manager

Die kontextbezogenen Startoptionen in Verbindung mit Log Insight werden im Dropdown-Menü **Aktionen** der vSphere-Benutzeroberfläche angezeigt. Sie können diese Menüelemente verwenden, um Log Insight zu öffnen und um Protokollereignisse von einem Objekt in vRealize Operations Manager zu suchen.

Welche kontextbezogene Startaktion verfügbar ist, hängt vom Objekt ab, das Sie im vRealize Operations Manager-Bestand auswählen. Der Zeitraum der Abfragen ist auf 60 Minuten vor dem Klicken auf eine kontextbezogene Startoption begrenzt.

Tabelle 1-2. Objekte in der vSphere-Benutzeroberfläche von vRealize Operations Manager und deren entsprechende kontextbezogene Startoptionen und -aktionen

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in Log Insight
World	Öffnen von vRealize Log Insight	Öffnet Log Insight.	Log Insight zeigt die Registerkarte Interaktive Analyse an.
vCenter Server	Öffnen von vRealize Log Insight	Öffnet Log Insight.	Log Insight zeigt die Registerkarte Interaktive Analyse an.
Datencenter	Suchen nach Protokollen in vRealize Log Insight	Öffnet Log Insight und übergibt die Ressourcen-namen aller Hostsysteme unter dem ausgewählten Datencenterobjekt.	Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Datencenters enthalten.

Tabelle 1-2. Objekte in der vSphere-Benutzeroberfläche von vRealize Operations Manager und deren entsprechende kontextbezogene Startoptionen und -aktionen (Fortsetzung)

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in Log Insight
Cluster	Suchen nach Protokollen in vRealize Log Insight	Öffnet Log Insight und übergibt die Ressourcen-namen aller Hostsysteme unter dem ausgewählten Clusterobjekt.	Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Clusters enthalten.
Hostsystem	Suchen nach Protokollen in vRealize Log Insight	Öffnet Log Insight und übergibt den Ressourcen-namen des ausgewählten Hostobjekts.	Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die den Namen des ausgewählten Hostsystems enthalten.
Virtuelle Maschine	Suchen nach Protokollen in vRealize Log Insight	Öffnet Log Insight und übergibt die IP-Adresse der ausgewählten virtuellen Maschine und den Ressourcennamen des verbundenen Hostsystems.	Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die die IP-Adresse der virtuellen Maschine und den Namen des Hosts, auf dem sich die virtuelle Maschine befindet, enthalten.

Wenn Sie auf der Registerkarte **Warnungen** eine Warnung auswählen und dann im Kontextmenü auf **Protokolle in Log Insight suchen** klicken, wird der Zeitraum auf eine Stunde vor dem Auslösen der Warnung begrenzt. Wenn beispielsweise eine Warnung um 14:00 Uhr ausgelöst wurde, zeigt die Abfrage in Log Insight alle Protokollmeldungen an, die sich zwischen 13:00 und 14:00 Uhr ereigneten. Dies hilft Ihnen, Ereignisse zu identifizieren, die die Warnung ausgelöst haben könnten.

Sie können Log Insight über Metrikdiagramme in vRealize Operations Manager öffnen. Der Zeitraum der Abfrage, die von Log Insight ausgeführt wird, entspricht dem Zeitraum des Metrikdiagramms.

HINWEIS Die Zeiten, die in Log Insight und den Metrikdiagrammen in vRealize Operations Manager angezeigt werden, können unterschiedlich sein, wenn die Zeiteinstellung der virtuellen Appliances unterschiedlich ist.

Kontextbezogener Start in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager



Das Symbol für kontextbezogenen Start wird zwar auf mehreren Seiten der benutzerdefinierten Benutzeroberfläche angezeigt, Sie können jedoch Log Insight nur von den Seiten aus starten, auf denen die Log Insight-Benachrichtigungseignisse angezeigt werden:

- Seite „Warnungen – Übersicht“.
- Seite „Warnung – Zusammenfassung“ einer Log Insight-Benachrichtigungswarnung.
- Widgets „Warnungen“ auf Ihren Dashboards, wenn eine Log Insight-Benachrichtigungswarnung ausgewählt ist.

Wenn Sie in der benutzerdefinierten Benutzeroberfläche ein Log Insight-Benachrichtigungseignis auswählen, können Sie unter zwei kontextbezogenen Startaktionen wählen.

Tabelle 1-3. Kontextbezogene Startoptionen und -aktionen in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager

Kontextbezogene Startoption in vRealize Operations Manager	Aktion in vRealize Operations Manager	Aktion in Log Insight
Öffnen von vRealize Log Insight	Öffnet Log Insight.	Log Insight zeigt die Registerkarte Dashboards an und lädt das Dashboard „vSphere-Übersicht“.
Suchen nach Protokollen in vRealize Log Insight	Öffnet Log Insight und übergibt den Bezeichner der Abfrage, die das Benachrichtigungsereignis ausgelöst hat.	Log Insight zeigt die Registerkarte Interaktive Analyse an und führt die Abfrage durch, die das Benachrichtigungsereignis ausgelöst hat.

Wenn Sie eine Warnung auswählen, die nicht von Log Insight stammt, enthält das kontextbezogene Startmenü das Menüelement **VM- und Hostprotokolle in vRealize Log Insight suchen**. Wenn Sie dieses Menüelement wählen, öffnet vRealize Operations Manager Log Insight und übergibt die Bezeichner des Objekts, das die Warnung ausgelöst hat. Log Insight verwendet die Ressourcenbezeichner, um eine Suche in den verfügbaren Protokollereignissen durchzuführen.

Deaktivieren des kontextbezogenen Starts für Log Insight in vRealize Operations Manager

Sie können den Log Insight-Adapter von der vRealize Operations Manager-Instanz deinstallieren, um mit Log Insight verbundene Menüelemente von der Benutzeroberfläche von vRealize Operations Manager zu entfernen.

Über die Benutzeroberfläche von Log Insight für Administratoren können Sie den kontextbezogenen Start deaktivieren. Wenn Sie nicht auf Log Insight zugreifen können oder die Log Insight-Instanz gelöscht wird, bevor die Verbindung mit vRealize Operations Manager deaktiviert wird, können Sie die Registrierung von Log Insight über die Administrations-Benutzeroberfläche von vRealize Operations Manager aufheben. Weitere diesbezügliche Informationen finden Sie in der Hilfe des Verwaltungsportals von vRealize Operations Manager.



VORSICHT Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von Log Insight. Wenn eine andere Log Insight-Instanz registriert wurde, nachdem Sie die Instanz, die Sie deaktivieren möchten, registriert haben, setzt die zweite Instanz die Einstellungen der ersten außer Kraft, ohne Sie zu benachrichtigen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.
- 3 Deaktivieren Sie das Kontrollkästchen **Kontextbezogenen Start aktivieren**.
- 4 Klicken Sie auf **Speichern**.

Log Insight konfiguriert die vRealize Operations Manager-Instanz so, dass diese den Log Insight-Adapter entfernt. Dieser Vorgang kann einige Minuten dauern.

Entfernen des Log Insight -Adapters aus einer vRealize Operations Manager - Instanz

Wenn Sie den kontextbezogenen Start für eine vRealize Operations Manager-Instanz aktivieren, erstellt Log Insight eine Instanz des Log Insight-Adapters in der vRealize Operations Manager-Instanz.

Diese Instanz des Adapters bleibt in der vRealize Operations Manager-Instanz, wenn Sie Log Insight deinstallieren. Dadurch werden die Elemente des Menüs für den kontextbezogenen Start weiterhin im Menü „Aktionen“ angezeigt und verweisen auf eine Log Insight-Instanz, die nicht mehr existiert.

Um den kontextbezogenen Start in vRealize Operations Manager zu deaktivieren, müssen Sie den Log Insight-Adapter aus der vRealize Operations Manager-Instanz entfernen.

Sie können das Befehlszeilendienstprogramm cURL verwenden, um HTTP-POST-Anfragen an vRealize Operations Manager zu senden.

Voraussetzungen

- Überprüfen Sie, ob cURL auf Ihrem System installiert ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

HINWEIS Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

Vorgehensweise

- 1 Führen Sie in cURL die folgende Abfrage für die virtuelle vRealize Operations Manager-Appliance aus, um den Log Insight-Adapter zu finden.

```
curl -k --user admin username:passwd
https://URL:443/HttpPostAdapter/OpenAPIServlet -d
"action=getRelationships&resourceName=Log Insight
Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer&
getChildren=true&getParents=false"
```

Dabei sind *admin username* und *passwd* die Anmeldedaten des Administrators und *URL* die IP-Adresse der vRealize Operations Manager-Instanz.

Die Abfrage liefert ein Ergebnis in folgendem Format:

```
resourceName=Log Insight Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer
```

Parents:

Children:

```
resourceName=Log Insight ServerLog Insight location&
adapterKindKey=LogInsight&
resourceKindKey=LogInsightLogServerHost&
identifiers=HOST::Log Insight location
```

Dabei ist *Log Insight location* der HOST-Wert des untergeordneten Objekts der abgefragten Ressource. Sie können diesen Wert im Befehl zum Entfernen der Adapterinstanz verwenden.

- 2 Führen Sie den folgenden Befehl aus, um den Log Insight-Adapter zu entfernen:

```
curl -k --user admin username:passwd https://URL:443/HttpPostAdapter/OpenAPIServlet -d
"action=addRemoveParentChildRelationship&parentResource=Log Insight Server&adapterKindKey=Log
Insight&
resourceKindKey=LogInsightLogServer&addFlag=false&
childResources=Log Insight ServerLog Insight location,LogInsight,LogInsightLogServer-
Host,HOST::Log Insight location"
```

Dabei sind *admin username* und *passwd* die Anmeldedaten des Administrators, *URL* die IP-Adresse der vRealize Operations Manager-Instanz und *Log Insight location* der Hostspeicherort der untergeordneten Ressource der Beziehung, die Sie entfernen möchten.

Elemente des kontextbezogenen Starts von Log Insight werden aus den Menüs in vRealize Operations Manager entfernt. Weitere Informationen zum kontextbezogenen Start finden Sie unter *Kontextbezogener Start von Log Insight* in der produktbezogenen Hilfe von Log Insight.

Aktivieren oder Deaktivieren der Datenarchivierung in Log Insight

Durch Datenarchivierung werden alte Protokolle aufbewahrt, die aus Speicherplatzgründen möglicherweise von der virtuellen Log Insight-Appliance entfernt werden könnten. Log Insight kann archivierte Daten als NFS-Mounts speichern.

Log Insight erfasst und speichert Protokolle in einer Reihe von 1-GB-Buckets auf der Festplatte. Ein Bucket besteht aus komprimierten Protokolldateien und einem Index. Es enthält alles, was zur Durchführung von Abfragen in einem bestimmten Zeitraum notwendig ist. Sobald die Größe eines Bucket 1 GB erreicht, unterbricht Log Insight die Speicherung, schließt alle Dateien und verschließt das Bucket.

Wenn die Datenarchivierung aktiviert ist, kopiert Log Insight beim Verschließen des Bucket die rohen komprimierten Protokolldateien aus dem Bucket in eine NFS-Partition. Vor der Aktivierung der Datenarchivierung verschlossene Buckets werden nachträglich nicht mehr archiviert.

HINWEIS Log Insight verwaltet den für Archivierungszwecke verwendeten NFS-Mount nicht. Wenn Systembenachrichtigungen aktiviert sind, sendet Log Insight eine E-Mail, wenn der NFS-Mount bald über keinen freien Speicherplatz mehr verfügt. Wenn der NFS-Mount nicht genügend freien Speicherplatz hat oder länger als die Aufbewahrungszeit der virtuellen Appliance nicht verfügbar ist, stellt Log Insight die Aufnahme neuer Daten ein, bis für den NFS-Mount genügend freier Speicherplatz vorhanden ist, der NFS-Mount verfügbar oder die Archivierung deaktiviert wird.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf eine den folgenden Anforderungen entsprechende NFS-Partition haben.
 - Die NFS-Partition muss Lese- und Schreibvorgänge für Gastkonten ermöglichen.
 - Für den Mount darf keine Authentifizierung erforderlich sein.
 - Der NFS-Server muss NFS v3 unterstützen.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insights als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.

- 2 Klicken Sie unter "Konfiguration" auf **Speicher**.
- 3 Aktivieren Sie das Kontrollkästchen **Datenarchivierung aktivieren**, geben Sie den Pfad zu einer NFS-Partition ein, auf der die Protokolle archiviert werden, und klicken Sie auf **Testen**, um die Verbindung zu überprüfen.

Wenn die Datenarchivierung aktiviert ist, werden alte Protokolldateien in der NFS-Partition gespeichert.

- 4 Klicken Sie auf **Speichern**.

HINWEIS Durch Datenarchivierung werden Protokollereignisse aufbewahrt, die aus Speicherplatzgründen von der virtuellen Log Insight-Appliance entfernt wurden. Von der virtuellen Log Insight-Appliance entfernte Protokollereignisse, die archiviert wurden, können nicht mehr durchsucht werden. Wenn Sie archivierte Protokolle durchsuchen möchten, müssen Sie diese in eine Log Insight-Instanz importieren. Weitere Informationen zum Importieren von archivierten Protokolldateien finden Sie unter „[Importieren eines Log Insight-Archivs in Log Insight](#)“, auf Seite 95.

Weiter

Stellen Sie nach dem Neustart von Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie im Thema über ESXi-Protokolle im *Log Insight-Administratorhandbuch*.

Aktivieren der Benutzerauthentifizierung über Active Directory

Log Insight verfügt über eine integrierte Authentifizierungsmethode, die Sie zur Benutzerauthentifizierung verwenden können.

Wenn Sie mithilfe der integrierten Authentifizierungsmethode neue Benutzerkonten erstellen, stellen Sie den Benutzern Kennwörter zur Verfügung, die sie für die Anmeldung bei Log Insight verwenden müssen.

Damit die Benutzer sich nicht mehrere Kennwörter merken müssen, können Sie die Unterstützung der Active Directory-Authentifizierung aktivieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **Authentifizierung**.
- 3 Aktivieren Sie das Kontrollkästchen **Active Directory-Unterstützung aktivieren**.
- 4 Geben Sie im Textfeld **Standarddomäne** einen Domänennamen ein.

Beispiel: **firmenname.com**.

HINWEIS Im Standarddomänen-Textfeld darf nicht mehr als eine Domäne eingegeben werden. Wird der Standarddomäne, die Sie angegeben haben, von anderen Domänen vertraut, verwendet Log Insight die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in den vertrauenden Domänen zu überprüfen.

- 5 Geben Sie die Anmeldedaten eines der Standarddomäne angehörenden Bindungsbenutzers ein.

Log Insight verwendet die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in der Standarddomäne und in Domänen, die der Standarddomäne vertrauen, zu überprüfen.

- 6 Klicken Sie auf **Speichern**.

Weiter

Erteilen Sie AD-Benutzern und -Gruppen Berechtigungen, um auf die aktuelle Instanz von Log Insight zuzugreifen. Weitere Informationen hierzu finden Sie unter „[Hinzufügen eines Active Directory-Benutzers zu Log Insight](#)“, auf Seite 24.

Konfigurieren des für Active Directory zu verwendenden Protokolls

Wenn sich Log Insight mit einem Active Directory verbindet, wird standardmäßig zunächst ein Nicht-SSL-LDAP-Verbindungsaufbau, und dann erforderlichenfalls ein SSL-LDAP-Verbindungsaufbau versucht.

Wenn Sie die Active Directory-Kommunikation auf ein bestimmtes Protokoll beschränken oder die Reihenfolge der für die Verbindungsversuche zu verwendenden Protokolle ändern möchten, müssen Sie zusätzliche Konfigurationen in der virtuellen Log Insight-Appliance vornehmen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden. Siehe „[Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance](#)“, auf Seite 8.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur virtuellen Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
- 2 Öffnen Sie die Datei `/usr/lib/loginsight/application/etc/loginsight-config-base.xml` zur Bearbeitung.

Wenn Sie einen VI-Editor verwenden, lautet der Befehl `vi loginsight-config-base.xml`.

- 3 Fügen Sie im Abschnitt **Authentication** die Zeile hinzu, die der Konfiguration entspricht, die Sie anwenden möchten:

Option	Beschreibung
<code><ad-protocols value="LDAP" /></code>	Speziell, um LDAP ohne SSL zu verwenden
<code><ad-protocols value="LDAPS" /></code>	Speziell für die ausschließliche Verwendung von LDAP mit SSL
<code><ad-protocols value="LDAP,LDAPS" /></code>	Speziell, um erst LDAP und dann LDAP mit SSL zu verwenden
<code><ad-protocols value="LDAPS,LDAP" /></code>	Speziell, um erst LDAPS und dann LDAP ohne SSL zu verwenden

Wenn Sie kein Protokoll auswählen, versucht Log Insight zunächst LDAP und dann LDAP mit SSL zu verwenden.

- 4 Speichern und schließen Sie die Datei.
- 5 Führen Sie den Befehl `service loginsight restart` aus.

Installieren eines benutzerdefinierten SSL-Zertifikats über die Log Insight -Web-Benutzeroberfläche

Standardmäßig installiert Log Insight ein selbstsigniertes SSL-Zertifikat auf der virtuellen Appliance.

Das selbstsignierte Zertifikat generiert Sicherheitswarnungen, wenn Sie eine Verbindung mit der Log Insight-Web-Benutzeroberfläche herstellen. Wenn Sie kein selbstsigniertes Sicherheitszertifikat verwenden möchten, können Sie ein benutzerdefiniertes SSL-Zertifikat installieren. Die einzige Funktion, die ein benutzerdefiniertes SSL-Zertifikat benötigt, ist „Ereignisweiterleitung über SSL“. Wenn Sie über ein Cluster-Setup mit ILB-Aktivierung verfügen, finden Sie unter „[Aktivieren des integrierten Lastenausgleichsmo-](#)
[duls](#)“, auf Seite 18 die spezifischen Anforderungen für das benutzerdefinierte SSL-Zertifikat.

HINWEIS Die Log Insight-Web-Benutzeroberfläche und das Log Insight Ingestion-Protokoll cfapi verwenden dasselbe Zertifikat für die Authentifizierung.

Voraussetzungen

- Stellen Sie sicher, dass Ihr benutzerdefiniertes SSL-Zertifikat die folgenden Anforderungen erfüllt.
 - Die Zertifikatsdatei enthält sowohl einen gültigen privaten Schlüssel als auch eine gültige Zertifikatskette.
 - Der private Schlüssel wird vom RSA- oder DSA-Algorithmus generiert.
 - Der private Schlüssel ist nicht durch einen Kennwortsatz verschlüsselt.
 - Falls das Zertifikat von einer Kette anderer Zertifikate signiert wurde, sind alle anderen Zertifikate in der Zertifikatsdatei enthalten, die Sie importieren möchten.
 - Der private Schlüssel und alle Zertifikate, die in der Zertifikatsdatei enthalten sind, müssen PEM-codiert sein. Log Insight unterstützt keine DER-codierten Zertifikate und privaten Schlüssel.
 - Der private Schlüssel und alle Zertifikate, die in der Zertifikatsdatei enthalten sind, müssen im PEM-Format vorliegen. Log Insight unterstützt keine Zertifikate im Format PFX, PKCS12, PKCS7 oder anderen Formaten.
- Verketteten Sie den gesamten Textkörper jedes einzelnen Zertifikats in einer einzelnen Textdatei in der folgenden Reihenfolge.
 - a Privater Schlüssel: *ihr_domänenname.key*
 - b Hauptzertifikat: *ihr_domänenname.crt*
 - c Zwischenzertifikat: *DigiCertCA.crt*
 - d Stammzertifikat: *TrustedRoot.crt*
- Die öffnenden und schließenden Tags jedes Zertifikats müssen in folgendem Format vorliegen.


```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 [Generieren einer Zertifizierungsanforderung](#) auf Seite 89
Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.
- 2 [Anfordern einer Signatur von einer Zertifizierungsstelle](#) auf Seite 90
Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.
- 3 [Verketten von Zertifikatsdateien](#) auf Seite 90
Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.
- 4 [Hochladen des signierten Zertifikats](#) auf Seite 91
Laden Sie Ihr signiertes Zertifikat über die Log Insight-Webschnittstelle hoch.
- 5 [Konfigurieren der SSL-Verbindung zwischen dem Log Insight-Server und den Log Insight Agents](#) auf Seite 91
Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

Generieren einer Zertifizierungsanforderung

Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.

Voraussetzungen

- Laden Sie das entsprechende Installationsprogramm für OpenSSL auf <http://www.openssl.org/related/binaries.html> herunter. Verwenden Sie das heruntergeladene OpenSSL-Installationsprogramm, um es auf Windows zu installieren.
- Bearbeiten Sie die Datei `openssl.cfg`, um weitere erforderliche Parameter hinzuzufügen. Stellen Sie sicher, dass der Parameter `req_extensions` im Abschnitt `[req]` definiert ist.

```
[req]
.
.
req_extensions=v3_req #
```

- Fügen Sie einen adäquaten Eintrag „Alternativer Antragstellername“ für den Hostnamen oder die IP-Adresse Ihres Servers hinzu, wie beispielsweise `server-01.loginsight.domain`. Für den Hostnamen können Sie kein Muster festlegen.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Vorgehensweise

- 1 Erstellen Sie einen Ordner, in dem Ihre Zertifikatsdateien gespeichert werden sollen, zum Beispiel `C:\Certs\LI-2.5`.

- Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus, um Ihren privaten Schlüssel zu generieren:

```
C:\Certs\LI-2.5>openssl genrsa -out server.key 2048
```

- Erstellen Sie eine Zertifizierungsanforderung, indem Sie den folgenden Befehl ausführen:

```
C:\Certs\LI-2.5>openssl req -new -key server.key -out server.csr
```

HINWEIS Dieser Befehl wird interaktiv ausgeführt und es werden Ihnen eine Reihe von Fragen gestellt. Ihre Antworten werden durch Ihre Zertifizierungsstelle überprüft. Ihre Antworten müssen den Angaben der mit der Eintragung Ihres Unternehmens verbundenen Rechtsdokumente entsprechen.

- Folgen Sie den Anweisungen auf dem Bildschirm und geben Sie die Informationen ein, die in Ihren Zertifikatsantrag aufgenommen werden.

WICHTIG Geben Sie im Feld „Common Name“ (Allgemeiner Name) den Hostnamen oder die IP-Adresse des Servers an, zum Beispiel **mail.your.domain**. Wenn Sie alle Subdomains einschließen möchten, geben Sie ***your.domain** ein.

Ihre Zertifizierungsanforderungsdatei `server.csr` wird generiert und gespeichert.

Anfordern einer Signatur von einer Zertifizierungsstelle

Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.

Vorgehensweise

- ◆ Senden Sie Ihre `server.csr`-Datei an eine Zertifizierungsstelle.

HINWEIS Beantragen Sie bei der Zertifizierungsstelle, Ihre Datei im PEM-Format codieren zu lassen.

Die Zertifizierungsstelle bearbeitet Ihre Anforderung und sendet Ihnen eine im PEM-Format codierte `server.crt`-Datei zurück.

Verketten von Zertifikatsdateien

Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.

Vorgehensweise

- Erstellen Sie eine neue `server.pem`-Datei und öffnen Sie sie in einem Texteditor.
- Kopieren Sie den Inhalt Ihrer `server.key`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- Kopieren Sie den Inhalt Ihrer `server.crt`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 4 Wenn die Zertifizierungsstellen Ihnen ein Zwischenzertifikat oder ein verkettetes Zertifikat ausgestellt haben, fügen Sie die Zwischenzertifikate oder verketteten Zertifikate im folgenden Format am Ende der öffentlichen Zertifikatsdatei an.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 5 Speichern Sie Ihre server.pem-Datei.

Hochladen des signierten Zertifikats

Laden Sie Ihr signiertes Zertifikat über die Log Insight-Webschnittstelle hoch.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **SSL-Zertifikat**.
- 3 Suchen Sie Ihr benutzerdefiniertes SSL-Zertifikat und klicken Sie auf **Öffnen**.
- 4 Klicken Sie auf **Speichern**.
- 5 Starten Sie Log Insight neu.

Weiter

Stellen Sie nach dem Neustart von Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie im Thema über ESXi-Protokolle im *Log Insight-Administratorhandbuch*.

Konfigurieren der SSL-Verbindung zwischen dem Log Insight -Server und den Log Insight Agents

Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

SSL-Hauptfunktionen

Das Verstehen der wesentlichen SSL-Funktionen kann Ihnen bei der ordnungsgemäßen Konfiguration von Log Insight Agents helfen.

Der Log Insight-Agent speichert Zertifikate und nutzt diese dann zur Verifizierung der Serveridentität bei allen Verbindungen mit einem bestimmten Server mit Ausnahme der allerersten Verbindung. Wenn sich die Serveridentität nicht bestätigen lässt, weist der Log Insight-Agent die Verbindung mit dem Server ab und vermerkt eine entsprechende Fehlermeldung im Protokoll. Die vom Agent empfangenen Zertifikate werden im Ordner cert gespeichert.

- Navigieren Sie unter Windows zu C:\ProgramData\VMware\Log Insight Agent\cert.

- Navigieren Sie unter Linux zu `/var/lib/loginsight-agent/cert`.

Wenn der Log Insight-Agent eine sichere Verbindung mit dem Log Insight-Server hergestellt hat, prüft der Agent das vom Log Insight-Server erhaltene Zertifikat auf seine Gültigkeit. Der Log Insight-Agent nutzt Stammzertifikate, denen das System vertraut.

- Der Log Insight Linux Agent lädt die vertrauenswürdigen Zertifikate von `/etc/pki/tls/certs/ca-bundle.crt` oder `/etc/ssl/certs/ca-certificates.crt`.
- Der Log Insight Windows Agent nutzt System-Stammzertifikate.

Wenn der Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein anderes gültiges, selbstsigniertes Zertifikat mit demselben öffentlichen Schlüssel empfängt, akzeptiert der Agent das neue Zertifikat. Dies kann bei der Neuerstellung eines selbstsignierten Zertifikats unter Verwendung desselben privaten Schlüssels, jedoch mit anderen Details, wie einem neuen Ablaufdatum, geschehen. Ansonsten wird die Verbindung abgewiesen.

Wenn der Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein gültiges, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat empfängt, ersetzt der Log Insight-Agent stillschweigend das neue akzeptierte Zertifikat.

Wenn der Log Insight-Agent das selbstsignierte Zertifikat empfängt, nachdem er ein von einer Zertifizierungsbehörde (CA) signiertes Zertifikat erhalten hat, wird es vom Log Insight Agent zurückgewiesen. Der Log Insight-Agent akzeptiert das selbstsignierte, vom Log Insight-Server empfangene Zertifikat nur bei der ersten Verbindung mit dem Server.

Wenn der Log Insight-Agent über ein lokal gespeichertes, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat verfügt und ein gültiges, von einer anderen vertrauenswürdigen Zertifizierungsbehörde (CA) signiertes Zertifikat erhält, wird dieses vom Agent zurückgewiesen. Sie können die Konfigurationsoptionen des Log Insight-Agents so modifizieren, dass dieser das neue Zertifikat annimmt. Weitere Informationen hierzu finden Sie unter „[Konfigurieren der Log Insight Agents-SSL-Parameter](#)“, auf Seite 93.

Erzwingen von Nur-SSL-Verbindungen

Sie können die Log Insight-Web-Benutzeroberfläche verwenden, um Log Insight Agents und die Ingestion-API so zu konfigurieren, dass nur SSL-Verbindungen mit dem Server zugelassen werden.

HINWEIS Die aktuelle Version von Log Insight unterstützt keine Syslog SSL-Verbindungen und funktioniert nur für die Log Insight-Ingestion-API.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **SSL**.
- 3 Aktivieren Sie unter „API Server SSL“ das Kontrollkästchen **SSL-Verbindung erforderlich**.
- 4 Klicken Sie auf **Speichern**.

Die Log Insight-API gestattet nur SSL-Verbindungen zu dem Server. Nicht-SSL-Verbindungen werden abgewiesen.

Konfigurieren der Log Insight Agents -SSL-Parameter

Sie können die Konfigurationsdatei des Log Insight Agent ändern, um entsprechend die SSL-Konfiguration zu ändern. Sie können einen Pfad zu den vertrauenswürdigen Stammzertifikaten hinzuzufügen und Sie können festlegen, ob Zertifikate vom Log Insight Agent akzeptiert werden usw.

Dieses Verfahren gilt sowohl für den Linux- als auch für den Windows-Log Insight Agents.

Voraussetzungen

Für den Log Insight Linux Agent:

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich bei dem Linux-System an, auf dem Sie Log Insight Linux Agent installiert haben. Öffnen Sie eine Konsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass VMware vRealize Log Insight Linux Agent installiert ist und ausgeführt wird.

Für den Log Insight Windows Agent:

- Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Log Insight Windows Agent installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der VMware vRealize Log Insight Agent-Dienst installiert ist.

Vorgehensweise

- 1 Navigieren Sie zu dem Ordner, der die Datei `liagent.ini` enthält.

Betriebssystem	Pfad
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 Öffnen Sie die Datei `liagent.ini` in einem beliebigen Texteditor.
- 3 Fügen Sie dem `[server]`Abschnitt der Datei `liagent.ini` die folgenden Schlüssel hinzu.

Schlüssel	Beschreibung
<code>ssl_ca_path</code>	Der Pfad zur Bundle-Datei der vertrauenswürdigen Stammzertifikate. Wenn nicht anders festgehalten, verwendet Log Insight Windows Agent System-Stammzertifikate. Log Insight Linux Agent versucht, vertrauenswürdige Zertifikate von <code>/etc/pki/tls/certs/ca-bundle.crt</code> oder <code>/etc/ssl/certs/ca-certificates.crt</code> zu laden.
<code>ssl_accept_any</code>	Legt fest, ob Zertifikate vom Log Insight-Agent akzeptiert werden. Die möglichen Werte sind <code>yes</code>, <code>1</code>, <code>no</code> oder <code>0</code>. Wenn der Wert auf „Ja“ oder <code>1</code> festgelegt ist, akzeptiert der Log Insight-Agent jegliche Zertifikate vom Server und richtet eine sichere Verbindung zum Versenden von Daten ein. Der Standardwert ist „Nein“. Hinweis Ist <code>ssl_accept_any</code> auf „Ja“ oder <code>1</code> festgelegt, akzeptiert der Log Insight-Agent Zertifikate ohne übereinstimmenden Common Name.

Schlüssel	Beschreibung
ssl_accept_any_trusted	Die möglichen Werte sind Ja, 1, Nein oder 0. Wenn der Log Insight-Agent über ein lokal gespeichertes, von einer vertrauenswürdigen Zertifizierungsbehörde signiertes Zertifikat verfügt und ein anderes gültiges Zertifikat empfängt, welches von einer anderen vertrauenswürdigen Zertifizierungsbehörde signiert ist, prüft er die Konfigurationsoption. Ist der Wert auf „Ja“ oder 1 festgelegt, akzeptiert der Agent das neue gültige Zertifikat. Ist der Wert auf „Nein“ oder 0 festgelegt, lehnt er das Zertifikat ab und beendet die Verbindung. Der Standardwert ist „Nein“.
ssl_cn	Das selbstsignierte Zertifikat Common Name. Der Standardwert ist VMware vCenter Log Insight. Sie können einen benutzerdefinierten Common Name festlegen, gegen den das Feld Common Name des Zertifikats geprüft werden muss. Der Log Insight-Agent überprüft das Feld Common Name des empfangenen Zertifikats gegen den Hostnamen, der für die Verbindung konfiguriert wurde, anhand des Schlüssels hostname im Bereich [server]. Gibt es keine Übereinstimmung, prüft der Agent das Feld Common Name gegen den Schlüssel ssl_cn in der Datei liagent.ini. Stimmen die Werte überein, akzeptiert der Log Insight-Agent das Zertifikat.

HINWEIS Die Schlüssel werden nur verwendet, wenn das Protokoll im Bereich [server] auf cfapi festgelegt ist und wenn SSL aktiviert ist.

- 4 Speichern und schließen Sie die Datei liagent.ini.

Beispiel: Konfiguration

Es folgt ein Beispiel für eine SSL-Konfiguration.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

Ändern des Standard-Zeitlimits für Log Insight -Websitzungen

Zur Gewährleistung der Sicherheit Ihrer Umgebung laufen Log Insight-Websitzungen nach 30 Minuten ab. Sie können das Zeitlimit erhöhen oder verringern.

Das Zeitlimit kann über die Web-Benutzeroberfläche geändert werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.

- 3 Geben Sie im Bereich „Browsersitzung“ ein Zeitlimit in Minuten an.
Der Wert -1 deaktiviert Sitzungszeitlimits.
- 4 Klicken Sie auf **Speichern**.

Format der Log Insight -Archivdateien

Log Insight archiviert Daten in einem bestimmten Format.

Log Insight speichert Archivdateien auf einem NFS-Server und organisiert diese in hierarchischen Verzeichnissen basierend auf der Archivierungszeit. Beispiel:

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

wobei es sich bei `/backup` um den NFS-Speicherort, bei `2014/08/07/16` um den Zeitpunkt der Archivierung, bei `bd234b2d-df98-44ae-991a-e0562f10a49` um die Bucket-ID und bei `data.blob` um die archivierten Daten für das Bucket handelt.

Die Archivdaten `data.blob` bestehen aus einer komprimierten Datei, die interne Log Insight-Codierung verwendet. Sie enthält den ursprünglichen Inhalt für alle im Bucket gespeicherten Nachrichten sowie die statischen Felder wie „timestamp“ und „host“. Name, Quelle und Anwendungsname.

Sie können archivierte Daten in Log Insight importieren, archivierte Daten in eine Rohtextdatei exportieren und Nachrichteninhalt aus Archivdaten extrahieren. Siehe „[Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON](#)“, auf Seite 96 und „[Importieren eines Log Insight-Archivs in Log Insight](#)“, auf Seite 95.

Importieren eines Log Insight -Archivs in Log Insight

In Log Insight archivierte Protokolle können über die Befehlszeile importiert werden.

HINWEIS Obwohl Log Insight historische und Echtzeitdaten gleichzeitig verarbeiten kann, empfiehlt es sich, für die Verarbeitung von importierten Protokolldateien eine separate Instanz von Log Insight einzusetzen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden.
- Stellen Sie sicher, dass Sie Zugriff auf den NFS-Server haben, auf dem die Log Insight-Protokolle archiviert werden.
- Vergewissern Sie sich, dass in der virtuellen Appliance für Log Insight genügend Speicherplatz für die importierten Protokolldateien vorhanden ist.

Der mindestens verfügbare Speicher in der Partition `/storage/core` der virtuellen Appliance muss mindestens 10-mal so groß sein wie das archivierte Protokoll, das importiert werden soll.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen.
- 3 Zum Importieren eines Verzeichnisses von archivierten Log Insight-Protokollen führen Sie folgenden Befehl aus.

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

HINWEIS Der Import der archivierten Daten kann je nach Größe des Importordners sehr lange dauern.

- 4 Schließen Sie die SSH-Verbindung.

Weiter

Sie können die importierten Protokollereignisse durchsuchen, filtern und analysieren.

Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON

Über die Befehlszeile können Sie ein Log Insight-Archiv in eine gewöhnliche reine Textdatei oder in das JSON-Format exportieren.

HINWEIS Dieses Verfahren richtet sich an erfahrene Benutzer. Die Befehlssyntax und Ausgabeformate können sich in späteren Versionen von Log Insight ohne Rückwärtskompatibilität ändern.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden.
- Vergewissern Sie sich, dass in der virtuellen Appliance für Log Insight genügend Speicherplatz für die exportierten Dateien vorhanden ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Erstellen Sie ein Archivverzeichnis in der vApp für Log Insight.

```
mkdir /archive
```
- 3 Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen, indem Sie folgenden Befehl ausführen.

```
mount -t nfs archive-fileshare:archive directory path /archive
```
- 4 Prüfen Sie den verfügbaren Speicherplatz in der vApp für Log Insight.

```
df -h
```
- 5 Exportieren Sie ein Log Insight-Archiv in eine reine Textdatei.

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory output-file
```


Beispiel:

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49 /tmp/output.txt
```
- 6 Exportieren Sie den Inhalt einer Log Insight-Archivmeldung in das JSON-Format.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-file.
```


Beispiel:

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49 /tmp/output.json
```
- 7 Schließen Sie die SSH-Verbindung.

Konfigurieren der Log Insight -Ereignisweiterleitung mit SSL

Sie können einen Log Insight-Server auf die Weiterleitung eingehender Ereignisse an ein Syslog- oder Ingestion-API-Ziel mit SSL konfigurieren.

Voraussetzungen

Die Ereignisweiterleitung mit SSL funktioniert nicht mit dem selbstsignierten Zertifikat, das standardmäßig auf den Zielservers installiert ist. Es muss ein benutzerdefiniertes SSL-Zertifikat erstellt und hochgeladen werden. Siehe [„Installieren eines benutzerdefinierten SSL-Zertifikats über die Log Insight-Web-Benutzeroberfläche“](#), auf Seite 88.

Vorgehensweise

- 1 Kopieren Sie das vertrauenswürdige Stammzertifikat in ein temporäres Verzeichnis auf der Weiterleitungsinstanz. Beispiel: /home.
- 2 SSH an die Weiterleitungsinstanz, und führen Sie die folgenden Befehle aus.

```
localhost:~ # cd /usr/java/jre1.7.0_51/lib/security/
localhost:/usr/java/jre1.7.0_51/lib/security # ../../bin/keytool -import -alias loginsight -
file /home/cacert.pem -keystore cacerts
```

Das Standard-Keystore-Kennwort ist **changeit**.

HINWEIS Java-Versionen können mit der Zeit variieren.

- 3 Starten Sie die Log Insight-Instanz neu.

Weiter

- Aktivieren Sie die SSL-Verbindung. Weitere Informationen hierzu finden Sie unter [„Erzwingen von Nur-SSL-Verbindungen“](#), auf Seite 92.
- Fügen Sie das Ziel für die Ereignisweiterleitung hinzu. Weitere Informationen hierzu finden Sie unter [„Hinzufügen eines Ziels für die Log Insight-Ereignisweiterleitung“](#), auf Seite 97.

Hinzufügen eines Ziels für die Log Insight -Ereignisweiterleitung

Sie können einen Log Insight-Server so konfigurieren, dass er neben dem Speichern und Indexieren von Ereignissen eingehende Ereignisse an ein Syslog- oder Ingestion-API-Ziel weiterleitet.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Ereignisweiterleitung**.

- 3 Klicken Sie auf **Neues Ziel**  und geben Sie die erforderlichen Informationen ein.

Option	Beschreibung
Name	Der eindeutige Name des neuen Ziels
Host	Die IP-Adresse oder der vollständig qualifizierte Domänenname
Protokoll	Ingestion-API oder Syslog. Die Standardeinstellung ist Ingestion-API.

- 4 (Optional) Fügen Sie Tags hinzu.

Mit Tags können Sie Ereignissen Felder mit vordefinierten Werten hinzufügen, um die Abfragen zu vereinfachen.

HINWEIS Tags sind nur im Zusammenhang mit der Ingestion-API verfügbar.

- 5 (Optional) Um die weitergeleiteten Ereignisse einzuschränken, klicken Sie auf  **Filter hinzufügen**.

Wenn Sie keinen Filter auswählen, werden alle Ereignisse weitergeleitet.

- 6 (Optional) Klicken Sie auf **Erweiterte Einstellungen anzeigen**, um die folgenden Weiterleitungseinstellungen zu ändern.

Option	Beschreibung
Port	Der Port, an den die Ereignisse im Remote-Ziel gesendet werden. Die Standardeinstellung wird anhand des angegebenen Protokolls festgelegt. Ändern Sie sie nur, wenn das Remote-Ziel einen anderen Port überwacht.
Festplatten-Cache	Die Menge an lokalem Festplattenspeicher, die zur Zwischenspeicherung der weiterzuleitenden Ereignisse reserviert wird. Die Zwischenspeicherung wird verwendet, wenn das Remote-Ziel nicht verfügbar ist oder die empfangenen Ereignisse nicht verarbeiten kann. Wenn der lokale Pufferspeicher voll und das Remote-Ziel noch nicht verfügbar ist, werden die ältesten lokalen Ereignisse gelöscht und nicht an das Remote-Ziel weitergeleitet, selbst wenn das Remote-Ziel wieder online ist. Die Standardeinstellung ist 200 MB.
Anzahl Worker	Die verwendete Anzahl gleichzeitiger ausgehender Verbindungen. Geben Sie eine höhere Anzahl von Workern an, um eine höhere Netzwerklatenz zum weitergeleiteten Ziel zu erreichen und mehr Ereignisse pro Sekunde weiterzuleiten. Die Standardeinstellung ist 2.

- 7 Klicken Sie zum Prüfen Ihrer Konfiguration auf **Test**.

- 8 Klicken Sie auf **Speichern**.

Weiter

Ereignisweiterleitungsziele können bearbeitet oder geklont werden.

Neustart des Log Insight -Dienstes

Sie können Log Insight über die Verwaltungsseite der Web-Benutzeroberfläche neu starten.



VORSICHT Bei einem Neustart von Log Insight werden alle aktiven Benutzersitzungen geschlossen. Benutzer der Log Insight-Instanz müssen sich erneut anmelden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Appliance**.
- 3 Klicken Sie auf **Master neu starten** und dann auf **Neu starten**.

Weiter

Stellen Sie nach dem Neustart von Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie im Thema über ESXi-Protokolle im *Log Insight-Administratorhandbuch*.

Ausschalten der virtuellen Log Insight -Appliance

Um beim Ausschalten eines Log Insight-Master- oder Worker-Knotens einen Datenverlust zu vermeiden, müssen Sie den Knoten in einer strengen Abfolge von Schritten ausschalten.

Sie müssen die virtuelle Log Insight-Appliance ausschalten, bevor Sie Änderungen an der virtuellen Hardware der Appliance vornehmen.

Sie können die virtuelle Log Insight-Appliance über die Menüoption **Betrieb > Gast herunterfahren** in vSphere Client, mithilfe der Konsole der virtuellen Appliance oder durch Herstellung einer SSH-Verbindung zur virtuellen Log Insight-Appliance und Ausführung eines Befehls ausschalten.

Voraussetzungen

- Wenn Sie eine Verbindung zu einer virtuellen Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.
- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Führen Sie zum Ausschalten der virtuellen Log Insight-Appliance `shutdown -h now` aus.

Weiter

Sie können sicher Änderungen an der virtuellen Hardware der virtuellen Log Insight-Appliance vornehmen.

Hinzufügen von Arbeitsspeicher und CPU zur virtuellen Log Insight -Appliance

Sie können die Arbeitsspeichermenge und die Anzahl der CPUs ändern, die einer virtuellen Log Insight-Appliance nach der Bereitstellung zugeteilt werden.

Sie müssen möglicherweise die Ressourcenzuweisung anpassen, beispielsweise wenn die Anzahl von Ereignissen in Ihrer Umgebung zunimmt.

Voraussetzungen

- Melden Sie sich bei vSphere Client als Benutzer mit Berechtigungen zum Ändern der Hardware der virtuellen Maschinen in Ihrer Umgebung an.
- Fahren Sie die virtuelle Log Insight-Appliance sicher herunter. Weitere Informationen hierzu finden Sie unter „[Ausschalten der virtuellen Log Insight-Appliance](#)“, auf Seite 99.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der vSphere Client-Bestandsliste auf die virtuelle Log Insight-Maschine und wählen Sie **Einstellungen bearbeiten** aus.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Passen Sie die CPU- und Arbeitsspeichermenge nach Bedarf an.
- 4 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn Sie die virtuelle Log Insight-Appliance einschalten, beginnt die virtuelle Maschine mit der Nutzung der neuen Ressourcen.

Einstellen des Versands von Protokollierungsdaten an VMware

Wenn Sie nicht mehr am Programm zur Verbesserung der Kundenzufriedenheit teilnehmen möchten, können Sie die Übertragung anonymisierter Protokollierungsdaten an VMware einstellen.

Sollten Sie Fragen oder Anliegen in Bezug auf das Programm zur Verbesserung der Kundenzufriedenheit für Log Insight haben, wenden Sie sich bitte an li-info@vmware.com.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.
- 3 Deaktivieren Sie im Bereich „Programm zur Verbesserung der Kundenzufriedenheit“ das Kontrollkästchen **Im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit wöchentliche Protokollierungsdaten an VMware senden**.
- 4 Klicken Sie auf **Speichern**.

Log Insight versendet keine Protokollierungsdaten mehr an VMware.

Fehlerbehebung bei Log Insight

Bevor Sie sich an die VMware Support-Dienste wenden, können Sie versuchen, allgemeine Probleme, die mit der Verwaltung von Log Insight in Zusammenhang stehen, selbst zu beheben.

Dieses Kapitel behandelt die folgenden Themen:

- „Es gehen keine ESXi-Protokolle mehr in Log Insight ein“, auf Seite 101
- „Log Insight steht zu wenig Festplattenspeicher zur Verfügung“, auf Seite 102
- „Herunterladen eines Support-Pakets für Log Insight“, auf Seite 103
- „Erstellen eines Support-Pakets von Log Insight über die Virtual Appliance-Konsole“, auf Seite 103
- „Zurücksetzen des Admin-Benutzerkennworts“, auf Seite 104
- „Zurücksetzen des Root-Benutzerkennworts“, auf Seite 104
- „Warnungen konnten nicht an vRealize Operations Manager gesendet werden“, auf Seite 105
- „Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich“, auf Seite 106
- „SMTP funktioniert bei aktivierter STARTTLS-Option nicht“, auf Seite 106
- „Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann“, auf Seite 107
- „Fehlschlagen des Upgrades mit einem internen Serverfehler“, auf Seite 108

Es gehen keine ESXi -Protokolle mehr in Log Insight ein

Nach einem Neustart des Log Insight-Dienstes gehen keine Syslog-Meldungen von ESXi-Hosts mehr in Log Insight ein.

Problem

Aufgrund von Konfigurationsänderungen in Log Insight ist ein Neustart des Log Insight-Dienstes erforderlich. Nach dem Neustart sind keine Syslog-Feeds von ESXi mehr verfügbar.

Ursache

Bestimmte ESXi-Versionen senden keine Protokolle mehr, wenn die Verbindung zum Remote-Syslog-Listener auch nur kurzzeitig unterbrochen wird. Dieses Problem betrifft je nach verwendetem Kommunikationsprotokoll die folgenden ESXi-Versionen:

Tabelle 2-1. ESXi-Versionen, die das Versenden von Syslog-Meldungen einstellen

Kommunikationsprotokoll	Betroffene ESXi-Version
TCP	■ ESXi 5.0.x ■ ESXi 5.1.x
UDP	ESXi 5.0 und 5.0 Update 1

WICHTIG Dieses Problem wurde in ESXi 5.1 Update 2 und ESXi 5.0, Patch ESXi500-201401401-BG, behoben. VMware empfiehlt Ihnen, das Update oder den Patch anzuwenden, um sicherzustellen, dass Ihre ESXi-Hosts das Versenden von Syslog-Meldungen an ihre Remote-Ziele nicht unterbrechen. Weitere Informationen finden Sie unter <https://www.vmware.com/support/vsphere5/doc/vsphere-esxi-51u2-release-notes.html> und [VMware ESXi 5.0, Patch ESXi500-201401401-BG: Updates esx-base \(2065691\)](#). Wenn Sie das Update oder Patch nicht anwenden möchten, verwenden Sie die folgende Lösung.

Lösung

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Klicken Sie bei jeder vCenter Server-Instanz, bei der der Link **ESXi-Syslog-Konfigurationsinformationen anzeigen** vorhanden ist, auf den Link **ESXi-Syslog-Konfigurationsinformationen anzeigen**.
- 4 Wählen Sie alle Hosts aus, die zuvor konfiguriert waren und klicken Sie auf **Konfigurieren**.

HINWEIS Der Konfigurationsvorgang kann einige Minuten dauern. Sie müssen diesen Vorgang bei jedem Neustart von Log Insight wiederholen. Weitere Informationen zu Syslog-Problemen und -Lösungen, siehe [VMware ESXi 5.x-Host sendet keine Syslogs mehr an den Remote-Server \(2003127\)](#).

Log Insight steht zu wenig Festplattenspeicher zur Verfügung

Die Speicherkapazität eines Log Insight-Master- oder Worker-Knotens kann möglicherweise überschritten werden, wenn Sie eine kleine virtuelle Festplatte verwenden und keine Archivierung aktiviert ist.

Problem

Log Insight steht zu wenig Festplattenspeicher zur Verfügung, wenn der Anteil der eingehenden Protokolle 3 Prozent des Speicherplatzes pro Minute überschreitet.

Ursache

Im Normalfall wird die Speicherkapazität von Log Insight nie überschritten, da jede Minute geprüft wird, ob der freie Speicherplatz weniger als 3 Prozent beträgt. Wenn der freie Speicherplatz auf der virtuellen Log Insight-Appliance unter 3 Prozent fällt, werden alte Daten-Buckets stillgelegt.

Ist die Festplatte jedoch klein und die Protokollaufnahmerate so hoch, dass der freie Speicherplatz (3 Prozent) innerhalb von 1 Minute vollständig in Anspruch genommen wird, wird die Speicherkapazität von Log Insight überschritten.

Bei aktivierter Archivierung archiviert Log Insight das Bucket vor dessen Stilllegung. Wenn der freie Speicherplatz voll belegt ist, bevor das alte Bucket archiviert und stillgelegt wurde, steht Log Insight zu wenig Festplattenspeicher zur Verfügung.

Lösung

- ◆ Erhöhen Sie die Speicherkapazität der virtuellen Log Insight-Appliance. Weitere Informationen hierzu finden Sie unter „[Erhöhen der Speicherkapazität der virtuellen Log Insight-Appliance](#)“, auf Seite 20.

Herunterladen eines Support-Pakets für Log Insight

Falls Log Insight aufgrund eines Problems nicht wie erwartet funktioniert, können Sie eine Kopie der Protokoll- und Konfigurationsdateien an die VMware Support-Dienste senden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

- 1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration  und wählen Sie **Verwaltung** aus.
- 2 Klicken Sie unter „Verwaltung“ auf **Appliance**.
- 3 Klicken Sie unter dem Support-Header auf **Support-Paket herunterladen**.
Das Log Insight-System erfasst die Diagnoseinformationen und streamt die Daten in einem komprimierten Tarball an Ihren Browser.
- 4 Klicken Sie im Dialogfeld „Datei-Download“ auf **Speichern**.
- 5 Wählen Sie das Verzeichnis aus, in dem Sie das Tarball-Archiv speichern möchten, und klicken Sie auf **Speichern**.

Weiter

Sie können den Inhalt der Protokolldateien auf Fehlermeldungen überprüfen. Wenn Sie Probleme behoben haben, löschen Sie das veraltete Support-Paket, um Festplattenspeicher freizugeben.

Erstellen eines Support-Pakets von Log Insight über die Virtual Appliance-Konsole

Wenn Sie nicht auf die Web-Benutzeroberfläche von Log Insight zugreifen können, können Sie mithilfe der Konsole der virtuellen Appliance oder nach Herstellung einer SSH-Verbindung zur virtuellen Appliance von Log Insight das Support-Paket herunterladen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden.
- Wenn Sie eine Verbindung zu einer virtuellen Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Führen Sie zur Erstellung des Support-Pakets `loginsight-support` aus.

Die Support-Informationen werden erfasst und in einer `*.tar.gz`-Datei mit der folgenden Benennungskonvention gespeichert: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, wobei `xxxxx` für die Prozess-ID steht, unter der der Prozess `loginsight-support` ausgeführt wurde.

Weiter

Leiten Sie das Support-Paket wie verlangt an die VMware Support-Dienste weiter.

Zurücksetzen des Admin-Benutzerkennworts

Wenn ein Admin-Benutzer das Kennwort für die Web-Benutzeroberfläche vergisst, ist das Konto nicht mehr erreichbar.

Problem

Wenn es nur einen Admin-Benutzer für Log Insight gibt und der Admin-Benutzer das Kennwort vergisst, kann die Anwendung nicht verwaltet werden. Wenn ein Admin-Benutzer der einzige Benutzer von Log Insight ist, kann auf die gesamte Web-Benutzeroberfläche nicht mehr zugegriffen werden.

Ursache

In Log Insight gibt es keine Benutzeroberfläche, in der Admin-Benutzer ihre eigenen Kennwörter zurücksetzen können, wenn ein Benutzer sich nicht an das aktuelle Kennwort erinnert.

HINWEIS Admin-Benutzer, die sich anmelden können, können das Kennwort anderer Admin-Benutzer zurücksetzen. Setzen Sie das Admin-Benutzerkennwort nur zurück, wenn von allen Admin-Benutzerkonten kein Kennwort bekannt ist.

Lösung

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden. Siehe „[Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance](#)“, auf Seite 8.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur virtuellen Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
- 2 Geben Sie `li-reset-admin-passwd.sh` ein und drücken Sie die **Eingabetaste**.

Das Skript setzt das Admin-Benutzerkennwort zurück, erstellt ein neues Kennwort und zeigt dieses auf dem Bildschirm an.

Weiter

Melden Sie sich mit dem neuen Kennwort bei der Web-Benutzeroberfläche von Log Insight an und ändern Sie das Admin-Benutzerkennwort.

Zurücksetzen des Root-Benutzerkennworts

Wenn Sie das Kennwort des Root-Benutzers vergessen, können Sie keine SSH-Verbindungen mehr herstellen oder die Konsole der virtuellen Log Insight-Appliance verwenden.

Problem

Wenn Sie keine SSH-Verbindungen herstellen oder die Konsole der virtuellen Log Insight-Appliance nicht verwenden können, können Sie bestimmte Verwaltungsaufgaben nicht ausführen und das Kennwort des Admin-Benutzers nicht zurücksetzen.

Lösung

- 1 Starten Sie in vSphere Client das Gastbetriebssystem der virtuellen Log Insight-Appliance und öffnen Sie die Konsole für die virtuelle Maschine.

- 2 Klicken Sie auf die Konsole, warten Sie, bis das GRUB-Menü angezeigt wird, und drücken Sie eine beliebige Buchstabentaste.

HINWEIS Die GRUB-Eingabeaufforderung wird 7 Sekunden lang auf dem Bildschirm angezeigt, bevor sie die Startsequenz anstößt.

- 3 Wählen Sie im GRUB-Menü mit den Pfeiltasten **SUSE Linux Enterprise Server für VMware**.

- 4 Drücken Sie die Leertaste, geben Sie **init=/bin/sh** ein und drücken Sie die Eingabetaste.

Der Kernel startet im Shell-Modus.

- 5 Geben Sie in der Shell **passwd** ein, drücken Sie die Eingabetaste und folgen Sie den Anweisungen auf dem Bildschirm, um das Root-Kennwort zu ändern.

Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen wie \$ oder & enthalten. Sie können dasselbe Zeichen nicht mehr als vier Mal wiederholen.

- 6 Geben Sie in der Shell **reboot** ein.

Weiter

Prüfen Sie, sobald Log Insight neu gestartet wird, ob Sie sich als Root-Benutzer anmelden können.

Warnungen konnten nicht an vRealize Operations Manager gesendet werden

Log Insight benachrichtigt Sie, wenn ein Warnungsereignis nicht an vRealize Operations Manager gesendet werden kann. Log Insight wiederholt das Senden der Warnung jede Minute, bis das Problem behoben ist.

Problem

In der Symbolleiste von Log Insight wird ein rotes Symbol mit einem Ausrufezeichen angezeigt, wenn eine Warnung nicht an vRealize Operations Manager übermittelt werden konnte.

Ursache

Aufgrund von Verbindungsproblemen kann Log Insight keine Warnungsbenachrichtigungen an vRealize Operations Manager versenden.

Lösung

- Klicken Sie auf das rote Symbol, um die Liste der Fehlermeldungen zu öffnen, und scrollen Sie nach unten, um die aktuellste Nachricht anzuzeigen.

Das rote Zeichen verschwindet von der Symbolleiste, wenn Sie die Liste der Fehlermeldungen öffnen oder das Problem behoben ist.
- Versuchen Sie, mit den folgenden Anweisungen das Verbindungsproblem mit vRealize Operations Manager zu beheben:
 - Stellen Sie sicher, dass die vRealize Operations Manager-vApp nicht heruntergefahren wurde.
 - Überprüfen Sie, ob Sie sich mit vRealize Operations Manager über die Schaltfläche **Verbindung testen** im Abschnitt **vRealize Operations Manager** der Seite **Verwaltung** der Log Insight-Web-Benutzeroberfläche verbinden können.
 - Stellen Sie sicher, dass Sie über die richtigen Anmeldedaten verfügen, indem Sie sich direkt bei vRealize Operations Manager anmelden.
 - Überprüfen Sie die Protokolle aus Log Insight und vRealize Operations Manager auf Meldungen, die auf Verbindungsprobleme hinweisen.

- Vergewissern Sie sich, dass keine Warnungen in der vRealize Operations Manager vSphere-Benutzeroberfläche herausgefiltert werden.

Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich

Sie können sich nicht bei der Web-Benutzeroberfläche von Log Insight anmelden, wenn Sie Active Directory-Anmeldedaten verwenden.

Problem

Sie können sich nicht mit Ihren Anmeldedaten für die Active Directory-Domäne bei Log Insight anmelden, obwohl ein Administrator Ihr Active Directory-Konto in Log Insight aufgenommen hat.

Ursache

Die häufigsten Ursachen hierfür sind abgelaufene Kennwörter, falsche Anmeldedaten, Verbindungsprobleme oder mangelnde Uhrzeitsynchronisation zwischen der virtuellen Log Insight-Appliance und Active Directory.

Lösung

- Vergewissern Sie sich, dass Ihre Anmeldedaten gültig sind, Ihr Kennwort nicht abgelaufen und Ihr Active Directory-Konto nicht gesperrt ist.
- Wenn Sie keine mit Active Directory-Authentifizierung zu verwendende Domäne angegeben haben, vergewissern Sie sich, dass in der Log Insight-Konfiguration unter `/usr/lib/loginsight/application/etc/loginsight-config-base.xml` ein in der Standarddomäne gespeichertes Konto vorhanden ist.
- Stellen Sie sicher, dass Log Insight über eine Verbindung zum Active Directory-Server verfügt.
 - Begeben Sie sich zum **Authentifizierungsabschnitt** der **Verwaltungsseite** der Log Insight Web-Benutzeroberfläche, geben Sie Ihre Anmeldedaten ein und klicken Sie auf die Schaltfläche **Verbindung testen**.
 - Überprüfen Sie, ob in Log Insight `/storage/var/loginsight/runtime.log` mit DNS-Problemen verbundene Meldungen vorhanden sind.
- Stellen Sie sicher, dass die Uhrzeiten in Log Insight und Active Directory zueinander synchron sind.
 - Überprüfen Sie, ob in Log Insight `/storage/var/loginsight/runtime.log` mit Taktverschiebungen verbundene Meldungen vorhanden sind.
 - Verwenden Sie einen NTP-Server, um die Uhrzeiten von Log Insight und Active Directory zu synchronisieren.

SMTP funktioniert bei aktivierter STARTTLS-Option nicht

Bei der Konfiguration des SMTP-Servers mit aktivierter STARTTLS-Option schlägt der Versand von Test-E-Mails fehl. Fügen Sie Ihr SSL-Zertifikat für den SMTP-Server dem Java-Truststore hinzu, um das Problem zu beheben.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen Log Insight-Appliance anzumelden.
- Wenn Sie eine Verbindung zu einer virtuellen Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Kopieren Sie das SSL-Zertifikat für den SMTP-Server in die Log Insight vApp.
- 3 Führen Sie den folgenden Befehl aus.

```
`/usr/java/latest/bin/keytool -import -alias zertifikat_name -file pfad_zum_zertifikat -key-store /usr/java/latest/lib/security/cacerts`
```

HINWEIS Die äußeren Anführungszeichen werden mit dem Gravis-Zeichen eingegeben, das sich auf Ihrer Tastatur auf derselben Taste befindet wie die Tilde. Verwenden Sie keine einfachen Anführungszeichen.

- 4 Geben Sie das Standardkennwort **changeit** ein.
- 5 Führen Sie den Befehl `service loginsight restart` aus.

Weiter

Gehen Sie auf **Verwaltung > Smtip** und testen Sie über **Test-E-Mail senden** Ihre Einstellungen. Siehe „[Konfigurieren des SMTP-Servers für Log Insight](#)“, auf Seite 68.

Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann

Log Insight-Upgrade schlägt aufgrund einer beschädigten PAK-Datei, einer abgelaufenen Lizenz oder nicht ausreichenden Festplattenspeichers fehl.

Problem

Das Upgrade von Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen. Fehler beim Upgrade: Signatur der PAK-Datei kann nicht validiert werden` wird angezeigt.

Ursache

Dieser Fehler kann die folgenden Ursachen haben:

- Bei der hochgeladenen Datei handelt es sich nicht um eine PAK-Datei.
- Die hochgeladene PAK-Datei ist nicht vollständig.
- Die Lizenz von Log Insight ist abgelaufen.
- Auf dem Root-Dateisystem der virtuellen Log Insight-Appliance ist nicht genügend Festplattenspeicher verfügbar.

Lösung

- Stellen Sie sicher, dass Sie eine PAK-Datei hochladen.
- Gleichen Sie „md5sum“ der PAK-Datei mit der VMware-Downloadsite ab.
- Stellen Sie sicher, dass mindestens eine gültige Lizenz für Log Insight konfiguriert ist.
- Melden Sie sich bei der virtuellen Log Insight-Appliance an und führen Sie `df -h` aus, um den verfügbaren Festplattenspeicher zu ermitteln.

HINWEIS Legen Sie keine Dateien im Root-Dateisystem der virtuellen Log Insight-Appliance ab.

Fehlschlagen des Upgrades mit einem internen Serverfehler

Aufgrund eines Verbindungsproblems schlägt das Log Insight-Upgrade mit einem internen Serverfehler fehl.

Problem

Das Upgrade von Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen. Interner Serverfehler` wird angezeigt.

Ursache

Es ist ein Verbindungsproblem zwischen dem Client und dem Server aufgetreten. Dies geschieht beispielsweise, wenn Sie versuchen, ein Upgrade von einem Client auszuführen, welcher sich in einem WAN befindet.

Lösung

- ◆ Führen Sie das LI-Upgrade von einem Client in demselben LAN wie der Server aus.

Index

A

- Abmeldung aller Benutzer **98**
- Active Directory
 - Benutzer **24**
 - Gruppen **25**
- Active Directory-Anmeldedaten **106**
- AD
 - Authentifizierung **86**
 - Benutzer **24**
 - Gruppen **25**
 - SSL **86, 87**
 - TCL **86**
- Adapter **78**
- Admin-Kennwort **104**
- Agent, mit Parametern installieren **30**
- Agent deinstallieren **45**
- Agent konfigurieren **43**
- Agent wird nicht angezeigt **55**
- Agent-Konfiguration **31**
- Agent-Massenbereitstellung **44**
- Agent-Massenugrade **44**
- Agent-StandardEinstellungen **31**
- Agent-Übersicht **28**
- Agents überwachen **22**
- aktualisieren
 - Befehlszeilenschnittstelle **11**
 - über Benutzeroberfläche **12**
- Anmeldung nicht möglich **106**
- API **92**
- Arbeitsspeicher hinzufügen **99**
- Archiv exportieren, Archiv nach JSON exportieren, Archiv in Textdatei exportieren **96**
- Aufgaben **71**
- Aufnahme Lastenausgleichsmodul **18**
- ausgehende Verbindung **57**
- Ausnahmeregel für den Ausgang **56**
- Ausschalten **99**

B

- Benachrichtigungen, Log Insight **77**
- Benachrichtigungsereignisse **69, 77**
- Benutzer, Verwaltung **22**
- Benutzeranmeldungen **23**
- benutzerdefinierte Zertifikate **88**

- benutzerdefiniertes SSL-Zertifikat, Hochladen **91**

- Benutzerkonten
 - löschen **28**
 - Neu **23**
- Benutzeroberflächen-Upgrade **12**
- Benutzerrolle ändern **27**
- Benutzerrolle erstellen **27**
- Benutzerrollen **27**
- Benutzerzugriff auf bestimmte Daten **26**
- Berechtigungen **23**
- Bereitstellung **13**
- Bereitstellung auf mehreren Computern **43**
- Bereitstellung der Appliance **13**
- Bereitstellung der virtuellen Appliance **13**

C

- Cluster, Clusterumgebung **61**
- Cluster aktualisieren **16**
- Cluster beitreten **15**
- Cluster verwalten **13**
- Clustermodus **15**
- CPU hinzufügen **99**

D

- Datenarchivierung **85**
- Datensatz **26**
- Debug-Protokollierungsebene **54**
- Debug-Protokollierungsebene ändern **54**
- Domänengruppen **25**
- Domänenkonto **24**

E

- E-Mail-Systemwarnungen **68**
- Ebene der Protokollierungsdetails **54**
- Effektive Agent-Konfiguration **40**
- Ereignisse, aus Windows-Ereigniskanal erfassen **34**
- Ereignisse aus Protokolldatei erfassen **38**
- Ereignisweiterleitung, Ereignisse an den Log Insight Windows Agent weiterleiten **42**
- Ereignisweiterleitung, Ereignisweiterleitung konfigurieren, Ereignisse weiterleiten **97**
- Erzwungene Abmeldung **98**
- ESXi konfigurieren **72**

ESXi-Konfiguration **72**
 exemplarische Agent-Konfiguration **40**
 Externes Lastenausgleichsmodul **61**

F

falsche Agent-Konfiguration **55**
 Fehlerbehebung
 ESXi-Protokolle **101**
 RPM-Paketupdate **58**
 Fehlerbehebung bei Log Insight Agents **54**
 Fehlerbehebung bei Log Insight Linux Agent **54**
 Fehlerbehebung bei Log Insight Windows Agent **54**
 Fehlerbehebung beim Agent **55, 58**
 Fehlerbehebung der Agent-Konfiguration **55**
 Fehlerbehebung für SMTP **106**
 Fehlerbehebung für STARTTLS **106**
 Festplatten hinzufügen **20**
 Firewall-Ausnahme hinzufügen **56**
 Firewall-Verbindung zulassen **57**
 Flatfile-Erfassung **38**

G

Gruppenrichtlinienobjekt **44**

H

Hinzufügen einer Suchdomäne **78**
 Horizontalskalierungs-Warnungen **65**
 Hostliste **21**
 Hostübersicht **21**
 Hostüberwachung **21**

I

Inhaltspaket **79**
 Installation **13**
 Integration
 vCenter Server **70**
 vRealize Operations Manager **76**
 vSphere **70**
 Integration von Log Insight **69**
 Integriertes Lastenausgleichsmodul **18**
 interner Serverfehler **108**
 IP-Adresse
 Ändern **9**
 Konfiguration **9**
 IP-Adresseinstellungen **9**

K

Kennwort
 Admin **104**
 root **104**
 Knoten aktualisieren **13, 16**
 Knoten entfernen **13, 17**

Konfiguration mehrerer Agents **40**
 Konfiguration von Linux-Agents **49**
 Konfigurationen zusammenführen **40**
 Kontextbezogenen Start deaktivieren **84**

L

Lastausgleich **72**
 LDAP SSL **87**
 Linux Agent
 BIN-Paket deinstallieren **53**
 BIN-Paket installieren **48**
 DEB-Paket deinstallieren **53**
 DEB-Paket installieren **47**
 Ereignisse aus Protokolldatei erfassen **50**
 Flatfile-Erfassung **50**
 RPM-Paket deinstallieren **52**
 RPM-Paket installieren **46**
 Übersicht **45**
 Zielserver festlegen **49**
 Linux Agent, Support-Paket **53**
 Lizenzierung **9**
 Log Insight
 Als Syslog-Server ausführen **72**
 Upgrade über Benutzeroberfläche, Upgrade auf Cluster **12**
 Log Insight Linux Agent **59, 61, 91**
 Log Insight Windows Agent **59, 61, 91**
 Log Insight-Adapter **78, 84**
 Log Insight-Agents **60, 93**
 Log Insight-Archivformat **95**
 Log Insight-Benachrichtigungen **77**
 Log Insight-Cluster, Worker-Knoten hinzufügen **13**

M

Massenbereitstellung **43**
 Massenbereitstellung fehlgeschlagen **58**
 Master-Knoten **15**
 mit Standardkonfiguration installieren **29**

N

Neustart wird durchgeführt **98**
 NFS **85**
 nicht verschlüsselter Datenverkehr **60**

P

PAK-Dateifehler **107**
 PEM-Datei, erstellen **90**
 Protokolldateien **103**
 Protokolle importieren **95**
 Protokollierungsdaten deaktivieren **100**

Protokollierungsdaten, Versenden einstellen **100**

Protokollimport **95**

Protokollrichtlinien **19**

Protokollweiterleitung

ESXi **72**

ESXi-Syslog **73**

syslog **74**

vCenter Server Appliance **75**

R

Rollen **23**

Rollenbasierte Zugriffssteuerung **22, 23, 26**

Root-Kennwort **8, 104**

Root-SSH **8**

rotes Zeichen in der Symbolleiste **105**

RPM-Paketupdate **58**

S

Selbstsigniertes Zertifikat **59**

Selbstsigniertes Zertifikat ablehnen **59**

Server weist die Verbindung ab **60**

Service, Neustart wird durchgeführt **98**

sichere Verbindung **91**

Sicherheitsmodell **22**

Sicherheitsrichtlinie **22**

signiertes Zertifikat, Hochladen **91**

SMTP **68**

SSH-Kennwort **8**

SSH-Root **8**

SSL **87, 97**

SSL-Funktionen **91**

SSL-Konfiguration **93**

SSL-Parameter **93**

SSL-Verbindung **60**

SSL-Verbindung erzwingen **92**

SSL-Verbindung konfigurieren **91**

SSL-Zertifikat für STARTTLS **106**

SSL-Zertifikate **88**

Standard-Zeitlimit **94**

Standardkonfiguration **31**

Start, kontextbezogen

Aktivieren **80**

deaktivieren **83**

Status **19**

Support-Paket **53, 103**

Support-Paket für den Windows Agent, Support-Paket **45**

syslog **72**

Syslog-Konfiguration **72**

Systembenachrichtigung **61**

Systembenachrichtigungen **62, 65**

Systemprotokolle **103**

Systemwarnungen **68**

Systemzustand **19**

Systemzustand der virtuellen Appliance **19**

U

Uhrzeitsynchronisierung **67**

Unterstützte Upgrades **10**

Upgrade mit Befehlszeilenschnittstelle **11**

Upgrade schlägt fehl **107, 108**

Upgrade-Pfade **10**

V

vCenter Server

Aufgaben **71**

Ereignisse **71**

Warnungen **71**

vCenter Server Appliance **75**

vCOPS-Integration **78**

Vergrößern des Speichers **20**

Versenden von Warnungen nicht möglich **105**

Verwaltung, Übersicht **7**

vRealize Operations Manager **69, 79**

vRealize Operations Manager-Inhaltspaket **79**

vSphere-Integration **70**

W

Warnungen **71**

Weiterleiten von Windows-Ereignissen **42**

Windows Agent **28, 29, 93**

Windows-Ereigniskanal

Ereignisfelder und Operanden **37**

Filter hinzufügen **35**

hinzufügen **34**

Worker aktualisieren **16**

Worker entfernen **17**

Worker hinzufügen **13**

Worker-Knoten **15**

Worker-Knoten, hinzufügen zu einem Cluster **13**

Z

Zeitlimit deaktivieren **94**

Zeitlimit der Sitzung **94**

Zeitlimit, deaktivieren **94**

Zeitüberschreitung, ändern **94**

zentrale Konfiguration **40**

Zertifikatsdatei, combine **90**

Zertifikatssignierungs-Anforderung, Generieren **89**

Zertifizierungsanforderung an eine Zertifizierungsstelle **90**

Zielgruppe **5**

Zielserver festlegen **33**
zu wenig Festplattenspeicher **102**
zu wenig Speicherplatz **102**